GSA e-Buy- Connect

My Rfqs | Close Connect Session

Modification Description

RFQ ID: RFQ949010 **Modification 1**

Date of Mod 1: 12/19/2014 05:03:22 PM EST

Description:
Amendment #1 (dated December 19, 2014): Contractor questions are due no later than January 9, 2015, 5:00 PM EST. This information is identified in the RFP (page 12). The Government will not respond to questions after January 9, 2015. The purpose of thi

Back

GSA e-Buy- Connect

My Rfqs | Close Connect Session

Modification Description

RFQ ID: RFQ949010 **Modification 2**

Date of Mod 2: 12/20/2014 10:59:06 AM EST

Description:
Amendment #2 (dated December 20, 2014): The purpose of this amendment is to identify the incumbent. The Incumbent is Heartland Technology Group (HTG). HTG is not a prime on the Alliant Small Business GWAC.

Back

GSA e-Buy- Connect

My Rfqs | Close Connect Session

Modification Description

RFQ ID: RFQ949010 **Modification 3**

Date of Mod 3: 01/15/2015 09:48:04 PM EST

Description:
Amendment #3: The closing date is changed to Feb. 20, 2015, 5:00 PM (EST). The Q&A document will be posted in a subsequent amendment within the next 1-2 weeks. Amendment #2 (dated December 20, 2014): The purpose of this amendment is to identify

Back

GSA e-Buy- Connect

My Rfqs | Close Connect Session

Modification Description

RFQ ID: RFQ949010 **Modification 4**

Date of Mod 4: 01/23/2015 03:23:30 PM EST

Description:
Amendment #4: Incorporates the Clarification document (Q&A), revised documents and clarification documents identified into the solicitation. Additional questions on Amendment #4 shall be submitted via email no later than January 30, 2015, 4:00 PM (CST).

▷ Back

GSA RFQ949010 (GSA Task Id ID05140054)
Amendment #4

Clarification Document dated 2015.01.23

The purpose of this clarification document is to address questions submitted in response to the Request for Proposal (RFP). The questions have not been altered. The clarification document will be incorporated into the resultant task order award. Furthermore, the release of the subject clarification incorporates the items listed below into the RFP. The revisions hereby replace previous versions of the same documents in their entirety.

Any additional questions resulting directly from the information provided via the release of the subject clarification document shall be submitted via e-mail to yjuania.still@gsa.gov and wendi.borrenpohl@gsa.gov no later than 4:00 PM CST January 30, 2015. All questions shall be submitted via a Microsoft Office Word file attached to the e-mail (questions within the body of an e-mail, a PDF file, an Excel file, or any other method/format will not be considered).

Clarification Document – Attachment A
Clarification Document – Attachment B
Clarification Document – Attachment C
Clarification Document – Attachment D
Clarification Document – Attachment E
Clarification Document – Attachment F
Clarification Document – Attachment G
RFP 2015.01.23 – revision 1
RFP Attachment 1 – PWS – 2015.01.23 – revision 1
RFP Attachment 1 – PWS Attachment A - 2015.01.23 – revision 1
RFP Attachment 1 – PWS Attachment B – 2015.01.23 - revision 1
RFP Attachment 2 – Pricing Template – 2015.01.23 - revision 1

1. Thanks for providing the incumbent contractor's name. My I know the incumbent contractor's contract number if possible?

   ***Answer:* The incumbent contractor is Heartland Technology Group LLC. The contract number is GS-06F-1249Z. The delivery order number is GSQ0514BM0085.**

2. In the RFP document, page 8, paragraph 3, b), "Furthermore, …… with an annual value of no less than $2 million." Will the Government consider remove the annual value restriction on past performance or reduce the annual value to no less than $1.6 million?

   ***Answer:* No.**

3. In RFP paragraph III.A.1, the Government states that the proposal documentation shall use "… Times New Roman font (no exceptions), no smaller than 11 point type-size …" May contractors use a smaller (but still legible) font in graphics and illustrations?

   ***Answer:* No.**

4. In RFP paragraph III.A.3, the Government provides a naming convention for the WinZip folders that will be uploaded, which includes the identifier "GS-06F-XXXXX". Contractors are asked to "Complete the X's with the GSA ASB contract number." The RFP cover has a contract number of "ID05140054", while the eBuy notice lists an RFQ ID of "RFQ949010." Neither of these numbers uses a "GS-06F" prefix. Will the Government please clarify which number contractors should use to complete the "X's" in the naming convention?

   ***Answer:* The contractor's Alliant Small Business (ASB) contract number (refer to emphasis placed within the question) should be used (not ID05140054 or RFQ949010).**

5. In RFP paragraph IV.A.3, the Government states that "Overall proposal content, excluding the pricing submission, shall be no more than 45 pages in length." May contractors exclude cover pages, tables of contents, lists of exhibits, and similar index material from the 45-page limit?

   ***Answer*: No; however, the standalone file containing the cover letter (reference Request for Proposal (RFP) paragraph [(III)(A)(3)] is excluded from the page limitation.**

6. In RFP paragraph IV.A.3, the Government states that "Overall proposal content, excluding the pricing submission, shall be no more than 45 pages in length." Is the 2-page cover letter also excluded from the 45-page limit?

   ***Answer*: Yes.**

7. In RFP paragraph IV.B.1.b, the Government states that "The prime contractor shall also provide information on any subcontractor proposed." Does this mean that the prime contractor should provide the same information for all subcontractors as is required from the prime contractor in paragraph IV.B.1.a (including CAGE, DUNS, TIN, etc.)?

   ***Answer*: Yes. As applicable, the information identified in (IV)(B)(1)(a) shall be identified for proposed subcontractors.**

8. In RFP paragraph IV.B.2.c.ii, the Government asks contractors to include "Resumes of proposed staffing for all key positions …" in the technical proposal. May these resumes be excluded from the 45-page limit?

   ***Answer*: No. It shall also be noted that resumes are only required for personnel proposed to fill key positions, as identified by the contractor.**

9. In RFP paragraph IV.B.2.c.iii, the Government asks contractors to include in the technical proposal "The identification of all proposed LCATs … and complete skill level descriptions from the ASB contract and any additional task specific supplemental requirements in terms of expertise (i.e. education) and experience (in terms of years of experience) that are being proposed to support task order performance." Because this list of labor categories and their complete descriptions may be quite long, will the Government allow contractors to exclude this LCAT information from the 45-page limit?

   ***Answer*: Yes; however, the contractor shall comply with the following restrictions and requirements: The identification of the proposed labor categories (LCATs) and the corresponding skill level descriptions from the ASB contract along with any additional task specific supplemental requirements being proposed by the contractor may be provided as an appendix to the technical proposal; however, such appendix shall ONLY include said information. Any additional information inserted within said appendix will NOT be considered for evaluation purposes. Furthermore, any additional task specific supplemental requirements being proposed by the contractor (i.e. those above and beyond the skill level requirements included within the existing ASB LCAT skill level descriptions) shall be identified with emphasis via the utilization of bold and italic font.**

10. In RFP paragraph IV.B.4.d, the Government states that "…future actions and uncertainty regarding continuing need may result in the requirement to reduce the duration of support provided via the FFP FTE positions or fractional FTE positions (if proposed)," and in RFP paragraph IV.B.4.f, the Government states that "The contractor shall clearly identify all costs, other than the standard billable labor hours expended by contractor resources in direct support of such requirements, associated with support provided under work hour category D." Is the Government willing to consider the addition of a T&M CLIN for surge or special projects that fall outside of the scope of this effort? If so, would the government consider extending the page count for the price proposal to allow for the inclusion of the contractor's hourly rate table?

Answer: ***The pricing requirements referenced in (IV)(B)(4)(d) and (IV)(B)(4)(f) are included for different purposes. Proposals shall not include proposed support for work that is considered to be "out of the scope" of this effort. The required use pricing template, RFQ Attachment 2, includes a sheet that requires the contractor to provide an hourly labor rate for each ASB LCAT (i.e. hourly rate table). Such inclusion will ensure maximum flexibility for future requirements.***

11. Can the Government describe the specific weighting assigned to the three evaluation factors listed in RFP paragraph V.B?

    Answer: ***Refer to RFP paragraph (VI)(A)(3).***

12. In the last paragraph of Section 1 in the PWS (RFP Attachment 1), the Government states that "Copies of all MOUs/SLAs/OLAs relevant to this task order that are in place at the time of award will be provided to the contractor." Will the Government provide copies of the MOUs/SLAs/OLAs before the bid submission deadline, at least for the FFP CLINs, so that contractors can have a better indication of the service levels to which they will be held accountable?

    Answer: ***The service level targets, by service, are identified in the publically available NITC Service Catalog (Refer to "Clarification Document – Attachment E"). The catalog provides an adequate representation of the overall service levels that NITC is responsible for delivering.***

13. In the second bullet of RFP paragraph IV.B.2.c.iv, regarding the contractor's description of "… the standard compensation package(s) that will be employed …", the Government states that "The discussion regarding benefits shall address extended vacations (those exceeding a one week duration)." This instruction seems to relate to the management of workload during extended employee absences, although it is presented in conjunction with a discussion of benefits. To clarify, is this instruction meant to request information regarding contractor's leave benefits and the quantity of leave granted to its employees, in the context of our compensation plan(s)?

    Answer: ***The contractor proposal shall clearly address the contractor's policies concerning extended vacations. There is no limitation regarding the scope of the contractor's response.***

14. In RFP paragraph I.C, the Government states that "For indicating the scope of work only, core initial staffing in terms of Full-Time-Equivalent (FTE) positions are identified in PWS Attachment C." For pricing purposes, must contractors propose to the Government-provided FTE estimates?

    Answer: ***No. The estimate was provided to be used as a "guide" designed to assist the contractor in developing the staffing plan and subsequent price proposal. Contractors may reflect a different number of positions from those provided in the estimate, as well as a different number of labor hours from those identified in RFP (IV)(B)(4)(b). The estimates were not intended to limit any contractor's ability to submit alternative solutions to accomplish task requirements. However, if a contractor quote differs significantly from the estimate; then, the contractor is instructed to provide a detailed description to explain the rationale for the deviation. Failure to provide a detailed explanation of any significant variations, will impact the Government's evaluation of the contractor's solution.***

15. In the third and fourth bullets of RFP paragraph IV.B.2.c.i, the Government states that the organization chart shall include "… names of known individuals proposed to perform and fill positions …" and "… citizenship status of all known individuals proposed to perform and fill positions." Per the Immigration Reform and Control Act of 1986 (IRCA), a contractor is not permitted to inquire about a prospective employee's citizenship status before making a formal offer of employment. With this in mind, will the Government consider revising the fourth bullet to read "For positions to be filled both by named individuals and by future identified proposed staffing, include a statement to illustrate the contractor's intent regarding U.S. citizenship status. In addition, the chart shall include the identification of the overall percentage, in numerical format, of proposed U.S. citizens and non-U.S. citizens."?

***Answer:* Refer to the referenced paragraph of the revised RFP for applicable changes. The information required is necessary to enable the complete evaluation of the contractor's proposed staffing plan, to include compliance with the security requirements identified in PWS paragraph 11.1.**

16. Ref. Paragraph III, Instructions to Contractors:

    a) III.A.1 stipulates a Times New Roman font with no exceptions. Would the government allow a sans serif font such as Arial to be used, in a readable size no smaller than 10 points, for proposal graphics?

    ***Answer:* No.**

    b) III.A.3 states that the proposal cover letter is to be submitted as a standalone document, but III.B.2. states that the cover letter is part of a complete technical proposal submission. Please confirm that the technical proposal may begin with a title page containing offeror information, followed by a copy of the proposal cover letter (still to be submitted separately), and still comply with the government's instructions.

    ***Answer:* The proposal shall be submitted in accordance with the instructions established within the RFP. It is not suggested that duplicate information be included within the overall submission.**

    c) Please confirm that the title page, cover letter copy, table of contents, executive summary, resumes, and past performance do not apply to the technical proposal 45-page limit.

    ***Answer:* Confirmation partially denied. As per the RFP, said information, with the exception of the standalone cover letter document/file, shall be included within the established page limitation.**

17. Ref. Paragraph IV, Proposal Content: IV.B.2.a.i., Technical Approach / Understanding and Methodology, instructs a high level of detail to be used in describing the technical approach and analytical techniques to accomplish each of the task requirements identified in the PWS. Within the main PWS document, the task requirements are covered in high-level objectives and scope descriptions that can reasonably be addressed within the 45-page limit. However, the PWS supplemental material describes the tasks required under the 29 CLINs in great detail. Does the government intend for offerors to address the detailed tasks listed within each of the 29 CLINs, and if so, will the government consider expanding the technical proposal page limit to 75 pages?

    ***Answer:* No, the page limitation remains the same. The contractor is not required to address each task identified within the Contract Line Item Number (CLIN) document (the separate tasks identified in paragraph 2, scope and duties, of each CLIN document); however, the contractor shall address the overall support requirements of each separate CLIN.**

18. Reference: RFP; Page 3: Paragraph I INTRODUCTION; Subparagraph C. Level of Support; third sentence: "To ensure maximum flexibility with respect to the optional growth support, the contractor shall include a complete price list identifying the proposed hourly labor rates for all ASB labor categories (LCATs), as reflected in the pricing template, that will be used as the pricing basis for all optional growth support." Reference: Attachment 2 – Pricing Template; ASB Rate – All CATS worksheet; This appears to be asking for a copy of the GWAC Rates. Question: How will discounts be applied to this rate sheet for the optional growth support?

    ***Answer:* The referenced sheet is not a request for a GWAC rate sheet. The sheet has been revised to reflect the display of proposed rate discounts. The previous version is hereby replaced with**

"RFP Attachment 2 – Pricing Template – Revision 1" via the release of the subject clarification document.

19. Reference: Instructions To Contractors, III.A.1: Regarding page limitations, the documentation shall be single-spaced, Times New Roman font (no exceptions), no smaller than 11 point type-size… Question: Will the Government permit 9 point Ariel for the graphics, organization chart and/or transition plan?

    Answer: No.

20. Reference: Instructions To Contractors, III.A.1. Questions:

    a) 3.1 Regarding page size, will the Government permit the use of 11x17 not only for the Organizational chart, but also for responses to 2.a.ii Implementation through Phase-In to Phase-Out Plans, and 2.b Quality Control Plan?

       Answer: No.

    b) 3.2 If it is permissible to use 11x17, will it count as 2 pages?

       Answer: Not applicable.

    c) 3.3 Are resumes of key personnel included in the page count?

       Answer: Yes.

    d) 3.4 Will the Government permit Past Performance references to be excluded from page count?

       Answer: No.

21. Reference: Business Size Standard. Question: If company that exceeds the size of a "small business" is a joint venture partner in a joint venture that is bidding through another Alliant SB JV, is this setup qualified to bid for this small business contract?

    Answer: Contractors, to include joint ventures, authorized to submit proposals are required to be current ASB prime contractors.

22. Reference: PWS 014 and 025. Question: Can the Government please provide further explanation of the difference in the services between PWS 014 - Application Integration Engineering Support Services and 025 Senior Application Engineering Services?

    Answer: The documented "experience and expertise requirements" for each CLIN lists the different skill sets and experiences required.

    CLIN 0014 requires support of existing and new customer application instances within established NITC hosting infrastructure. CLIN 0014 requires knowledge of operating systems as well as COTS and other application packages supported by NITC. The contracted shall interface with the customer to ensure application performance and customer expectations are met.

    CLIN 0025 requires the contractor to assume an elevated role in transitioning customer applications to NITC supported infrastructure. CLIN 0025 requires a wider range of skills than those required for CLIN 0014. CLIN 0025 requires knowledge of security (e.g., firewall rule establishment, secure transport), networking (to include bandwidth determinations and routing), operation systems, application and data base, and customer interface skills. CLIN 0025 requires work between the customer application requirements and the various skill sets/subject matter expertise areas within NITC to effectively transition customer applications.

23. General Question: Since Phil Gehrt is shown as the author of the "Contractor In-Processing" and "Contractor Exit Process," will the Government please explain what Phil's role is in authoring this

RFP package? Through the vendor community, we understood that he was leading the contract acquisition process for the incumbent, while serving as a consultant for Armstrong and Associates, and that his son is a direct employ of the incumbent JMA IT. If he is also involved in authoring any part of the RFP, this would seem to be a conflict of interest.

<u>Answer</u>**:** ***The referenced documents were authored by Mr. Gehrt at a time when he was a Government employee. Mr. Gehrt has had no involvement with the RFP.***

24. Please be advised, three (3) of the CLIN documents (CLIN 009, 010 and 019) in the RFP, Attachment 1 – PWS Attachment A, do not reflect the correct CLIN Number in document.

    Answer: ***The CLIN documents have been reviewed and it was confirmed that updates to include/correct the CLIN identification within the CLIN 009, 010 and 018 were required. The previous version of "RFP Attachment 1 – PWS Attachment A" is hereby replaced with "RFP Attachment 1 – PWS Attachment A – Revision 1" via the release of the subject clarification document.***

25. To ensure that offerors can sufficiently address the Governments PWS requirements, would the Government please consider excluding the Past Experience & Performance section from the 45 page limit? Thus, allow the offer to address it the Past Experiences & Performance section by setting a page limit not to exceed 10 pages?

    Answer: ***No.***

26. Will the Government allow offerors to use a different and small font for Graphics and Tables, such as Arial Narrow 10pt?

    Answer: ***No.***

27. On page 10 of the RFP, paragraph 8.6, it is stated that the monthly status report must include the status of task directives. Can you describe what a task directive is and how these will be issued to the contractor?

    Answer: ***A task directive is a method of documenting contractor tasks that are assigned to the contractor. Task directives will be issued by authorized Government representatives.***

28. On page 15, paragraph 9.5.2, within what time period must the non-standard duty hours be offset? Must these hours be offset within the week, month, quarter, year? How will it be handled if the non-standard work hours occur on the last day of the month, or after the employee has already worked the full monthly allocation?

    Answer: ***The off-set shall be completed within the same monthly reporting period, unless the non-standard duty work hours are expended in the last week of the monthly reporting period. Non-standard duty work hours expended within the last week of the monthly reporting period shall be off-set within the first two weeks of the following reporting period.***

29. RFP, paragraph IV.A..3 & IV.B.2.c.ii, pages 5&7. Are resumes for Key Personnel included as part of the 45 pg count? We believe that inclusion of the resumes in the page count will either restrict the number of Key Personnel, or reduce space for valuable technical discussion.

    Answer: ***Yes. Key personnel resumes are included within the established page limitation.***

30. RFP, paragraph IV.B.2.i, page 6. Please provide a definition for "Key Personnel".

    Answer: ***Key personnel are personnel proposed to perform in key positions. The contractor is responsible for identifying the key positions included within the contractor's respective staffing***

plan. Key positions are those deemed essential for successful contractor accomplishment of the work to be performed.

31. RFP, paragraph, V.B, page 9. Is there a weighting difference between Factors 1, 2 and 3 or are they weighted equally?

    Answer: ***Refer to RFP paragraph (VI)(A)(3).***

32. CLIN 029, paragraph, 2.c, page 1. On what platform is BMC ProActiveNet Performance Management (BPPM) system installed?

    Answer: ***BPPM is built on a windows platform.***

33. CLIN 1-29, Perfomance standards table, Var pages. What at grammatical standards are we being held to; i.e. Strunk and White, NYT etc.?

    Answer: ***The U.S. Government Printing Office (GPO) Style Manual (located at http://www.gpo.gov/fdsys/pkg/GPO-STYLEMANUAL-2008/content-detail.html) will be the primary governing guideline/instruction. Per the GPO Style Manual 2008, page V, "It should be remembered that the GPO Style Manual is primarily a GPO printer's stylebook. Easy rules of grammar cannot be prescribed, for it is assumed that editors are versed in correct expression. Likewise, decisions on design and makeup are best determined by the individual publisher to meet the needs of the intended audience." Pages 1-220 of the manual provide an adequate representation of Government requirements. It is highly recommended that all documents be proofread prior to submission to reduce the risk of AQL violations associated with grammatical requirements. The previous version of "RFP Attachment 1 – PWS Attachment B" is hereby replaced with "RFP Attachment 1 – PWS Attachment B – Revision 1" via the release of the subject clarification document to incorporate the identification of additional violations.***

34. CLINs 1-29, Performance standards table, Var. pages. Payment reductions are based on percentages such as 1%, 2% etc., what are those percentages connected to? There are no contract deliverables defined in the pricing volumes that are connected to any performance standards.

    Answer: ***The disincentive amount (i.e. payment reduction) will be calculated based on the total monthly CLIN price.***

35. RFP, III.A.4 & IX, pages 4 and 12. RFP Section III.A.4 states,"Hard copy proposals are to be delivered to the address listed in paragraph IV no later than 24 hours following the close date/time identified in the same paragraph." Section IX specifies, "Electronic proposals must be submitted no later than the date established in the eBuy, with six hardcopies to be delivered within 24 hours of this date/time…" The date/time in eBuy is January 30, 2015 at 5PM EST which is a Friday. Since the requirement for hardcopies to be delivered within 24 hours of the electronic submission would result in a Saturday delivery, request that the Government consider extending the due date of the hardcopies until Monday, February2, 2015 at 5PM EST.

    Answer: ***The delivery requirement for the hard copies is hereby changed to read "no later than the first business day following the close date/time established in eBuy".***

36. RFP, paragraph IV.A.3, page 5. Are the proposal cover sheets and table of contents for each volume excluded from the maximum page limitations for each volume?

    Answer: ***No.***

37. RFP, paragraph IV.A.3 & IV.B.1, page 5. RFP Section IV.A.3 states, "Overall proposal content, excluding the pricing submission, shall be no more than 45 pages in length." Is the Cover Letter (RFP Section IV.B.1) also excluded from the 45-page limitation?

Answer*:** ***Yes. The standalone file containing the cover letter is excluded from the page limitation.

38. RFP, paragraph IV.B.2.b, page 6. To enable offerors to provide sufficient detail to address the technical requirements, request that the Quality Control Plan be included as an Appendix to the Technical Volume and excluded from the 45-page response limitation.

    Answer*:** ***No.

39. Attachment 1, PWS Attachment A, paragraph 4, page 3. The Acceptable Quality Level (AQL) states that grammatical errors shall count as a violation, equal to that of delayed delivery. Which grammatical standard, or standards, has the USDA selected for judging whether or not an error has been committed (e.g. Strunk and White, AP Stylebook, MLA Handbook, Microsoft Manual of Style)?

    Answer*:** ***Refer to the response to question #33.

40. Attachment 1, PWS Attachment A, paragraph 4, page 3. The Incentive/Disincentive column speaks of "…a payment reduction of 1% up to the maximum reduction of…" As there are no provisions in the RFP for pricing of individual deliverables, what is the Payment from which the 1% is to be deducted, the total contract value, the CLIN value, a monthly invoice value or some other value?

    Answer*:** ***The disincentive amount (i.e. payment reduction) will be calculated based on the total monthly CLIN price.

41. RFP, paragraph IV.B.2.c.iii. To enable the offeror to provide sufficient detail regarding the labor category (LCAT) descriptions for key and non-key personnel, request that the Government permit the proposed LCATs, complete skill level descriptions from the ASB contract and any additional task-specific supplemental requirements in terms of expertise and experience to be included in an appendix excluded from the maximum page count limitation.

    Answer*:** ***Refer to the response to question #9.

42. PWS, paragraph 1, page 4. Paragraph 3 within PWS Section 1 talks about the use of the BMC Remedy ITSM suite under the direction of the ECCB for tool implementation. Does the government intend to remain with the Remedy offering or is it looking at alternative solutions going forward?

    Answer*:** ***Yes, NITC intends to continue utilizing the BMC software suite of products.

43. PWS, paragraph 2, Objective 4, page 5. Objective 4 mentions that the contractor is to provide support to NITC data center officials in the preparation of documentation for the NITC Change Control Board. Request that the Government please list what documentation is required to be supported and the CLIN under which this support is provided?

    Answer*:** ***Applicable training and documentation required to familiarize the contractor with the NITC Change Management requirements will be provided after issuance of task order award. This objective primarily refers to the contractor properly submitting Requests for Change and obtaining approval via the ITSM System (Remedy) before executing any work activities.

44. Section III. The solicitation calls for TimesNewRoman 11 without exception for all proposal content. We have an ISO-certified process that is explained by a complex image. We request a font exception for figures and tables to allow for TimesNewRoman 10 in tables and legible font in figures.

    Answer*:** ***Request denied.

45. Section IV.A.3. Please confirm that proposal front matter (i.e., forwarding letter, cover, table of contents, and compliance matrix) are not included in the 45 page limit.

    Answer*:** ***Confirmation partially denied. The standalone file containing the cover letter is excluded from the page limitation. All other documentation is included within the page limitation.

46. Section IV.A.3. Given the broad scope of requirements, detail requested in the technical response, number of key personnel, and number of labor categories, request Key Personnel resumes (RFQ IV.B.2.ii) and Labor Category Descriptions (RFQ IV.B.2.iii) be excluded from the page count.

    <u>Answer</u>: Key personnel resumes shall be included with the established page limitation. Refer to the response to question #9 for applicable information regarding LCAT documentation.

47. Section IV.B.2.C. This sections calls for an extensive organization chart that depicts a complete staffing approach/plan and extensive detail regarding each proposed individual (i.e., key/non, key, name, citizenship, contractor company, and ASB labor category). We believe the details re: all individuals would be better presented in a staffing table as opposed to being included in an organization chart. Please confirm a combination of an org chart and supporting staffing table is acceptable as opposed to forcing all of this information onto an org chart and can be presented on the same sheet where the page size in exempted from those defined in the proposal instructions.

    <u>Answer</u>: The requirements for the organizational chart remain unchanged. Per RPF paragraph (III)(A)(1), there is no page size limitation for the organization chart.

48. Section IX. Due date calls for electronic proposals to be submitted via eBuy, with six hard copies delivered within 24 hours to the specified address. We note that 24 hours later is a Saturday. Is the requirement 24 hours or 1 business day?

    <u>Answer</u>: Refer to the response to question #35.

49. CLINs 009, 011, & 18 Please check the numbering/titles of CLIN files 9, 10, and 18. Within the document for the file entitled “CLIN 009-2014.12.18-Program and Project Management”, this is the only document where the CLIN number is not in the title within the document. The title is listed as “Program/Project Management Support Services”. CLIN 0010-2014.12.18-Task Order Management, the title within the document is “CLIN –009-Task Order Management”. We believe this should be “CLIN 010….” CLIN 0018-2014.12.18-Network Engineering Services, the title within the document is “CLIN –017-Network Engineering Services”. We believe this should be “CLIN 018….”

    <u>Answer</u>: Refer to the response to question #24.

50. Is there an existing Concept of Operations by which PWS services are currently being performed? If so, will NITC provide the CONOPS as a reference for offerors?

    <u>Answer</u>: NITC does not have a CONOPS document. As an enterprise data center and cloud service hosting provider, NITC maintains several operational directives, manuals, procedures, and guides, etc., that will be made available after issuance of task order award.

51. PWS - Page 4 Objective 1 states that "the Contractor shall work as a part of the technical support team..." Which support tasks (i.e., CLINS) are performed by the Government versus the NITC contractor?

    <u>Answer</u>: The terminology “technical support team” refers to the overall NITC organization that provides comprehensive support services to NITC clients. All tasks identified within the Performance Work Statement (PWS) shall be performed by the contractor.

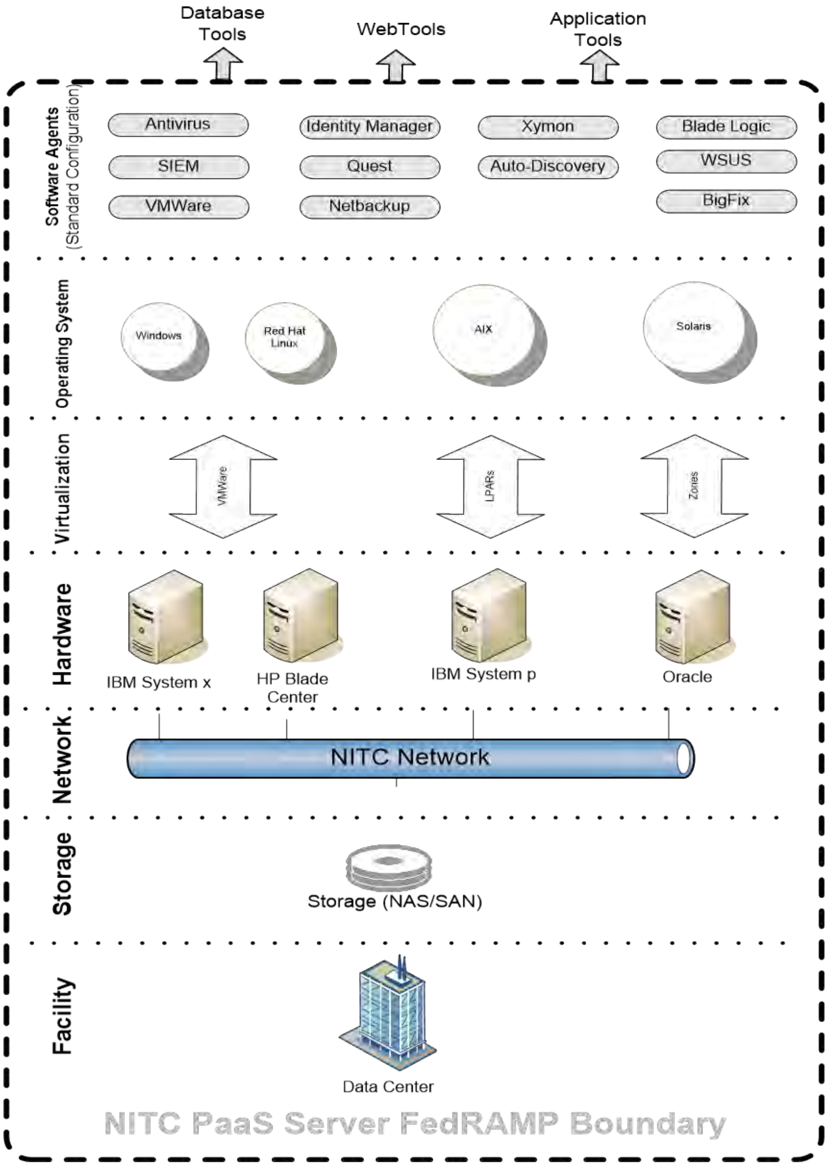
52. PWS Page 4 Background. Will the Government provide a description of the FedRamp Cloud Technologies and environment that will be managed as part of this contract?

    <u>Answer</u>: NITC utilizes advanced server virtualization technologies, strict standards, and economies of scale to facilitate a cloud hosting environment with the capability of hosting multiple virtual data centers and operating platforms. Virtualization alongside the highly available network provides the customers with many advantages over a typical physical computing environment

including, but not limited to, faster processing, greater up-time and redundancy. The two distinctive service offerings for virtualization for NITC are as follows:

- ***The NITC PaaS Server offering provides customers fully managed virtualized operating platform infrastructure up to and including one of the supported Operating Systems (Windows, Red Hat Linux, Solaris, and AIX). In addition to full platform administration, NITC is responsible for server software agents and auxiliary support resources including monitoring, audit logging and consolidation, virus scanning, central authentication, patching, and vulnerability detection. To protect this shared environment in regards to the Operating System, NITC must maintain control of elevated privileges. NITC PaaS Server services are fully integrated with NITC network, storage, and backup infrastructure. Customers are responsible for maintaining management control over their deployed applications.***
- ***The NITC IaaS Virtual Data Center (VDC) offering provides standard increments of resource quota to customers for the purpose of building and using their own VDCs and Virtual Machines (VMs). This allows multiple customers to provision virtual processing, storage, and other fundamental computing resources on hosted infrastructure. Customers are then able to deploy and run arbitrary software, including operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over their operating systems, storage, and deployed applications; and limited control of select networking components (e.g., host firewalls). The system relies on a highly-available design incorporating several technologies for providing the infrastructure, including VMWare and OpenStack. Within this component of the system, NITC provides and manages the platform external to the customer's VDC. Within their environment, customers can deploy and manage their own virtual machines.***

The NITC Infrastructure General Support System (NITC Infrastructure) includes VMWare and OpenStack components and hardware. The schematic embedded below should help to illustrate the technologies that comprise this environment.



53. PWS Page 4 Background. There are various Service type agreements referenced that may impact the required staffing levels to support the contract. Request the Government provide sample of the referenced agreements or be provided with an example of the SLAs and OLAs or a table outlining the agreements the contractor will need to adhere.

    <u>Answer</u>*: The requested information is not authorized to be released prior to issuance of task order award. The referenced agreements between the NITC and its customers will not be incorporated into the resultant task order award. The majority of the CLINs that will provide direct support related to NITC's compliance with established service level agreements are labor hours CLINs, which are considered to present lower staffing risk to the contractor. Refer to "Clarification Document – Attachment E" and "Clarification Document – Attachment F" for information pertaining to service level metrics (Attachment E) and service delivery requirements for incidents and service requests (Attachment F).

54. PWS Page 5 Objectives. Objective 5 references the attainment of services to provide seamless implementation and coordination of federal mandates. Request the Government provide a description of the scope of the desired coordination and involvement in to support federal mandates.

***Answer:** Adhering to federal mandates is achieved in many ways. An example is as follows: All USDA employees and contractors are required to use the LincPass/PIV card to obtain access to Government issued workstations and network access (i.e., a federal mandate). CLIN task assignments and the completion of these tasks will often support the Government in achieving federal mandates. An additional example includes CLIN task assignments associated with the upgrade of network protocols from IPV 4 to IPV6, which achieve federal mandates.*

55. PWS Page 5. Scope Does the Government have any ongoing initiatives or plans to transition away Legacy technologies that can be shared?

    ***Answer:** NITC does plan to transition from legacy equipment, where possible. However, support for legacy equipment is determined by customer requirements for continued maintenance.*

56. PWS Page 6 The link provided as a referenced to access applicable documents does not work. Does the Government have another web link to the Wiki site that can be used? (http://wiki.edc.usda.gov/mediawiki/index.php/Main_Page)

    ***Answer:** Documentation available for release prior to issuance of task order award can be obtained from the following link: http://www.ocio.usda.gov/about-ocio/data-center-operations-dco. Access to the identified wiki will be made available after the issuance of task order award.*

57. CLIN 11. Objective 2b requires "Creation of highly detailed documents which detail business requirements and how they relate to technical designs, specifications and solutions; to include development of technology roadmaps, technological standards, white papers, and complex architectural and infrastructural design documents."

    a) Does the Government require resources that will help with obtaining value from existing architecture and capabilities or should focus be on creating new capabilities that meet Government directives that may extend beyond the scope of this procurement?

       ***Answer:** It is anticipated that skill sets capable of completing each of the referenced tasks will be required.*

    b) Does the Government require resources that are capable of providing platform and/or application automation and orchestration service designs?

       ***Answer:** The referenced skills are not identified within the requirement documents; however, such skills may present added capabilities that could be leveraged based on customer needs.*

58. CLIN 25. Requirement 2g states that contractor must "Ensure customer access requirements to application target architecture are operational and meet customer requirements." Does the Government require applications to be moved to target environments with minimal changes or will application re-architecture be in scope?

    ***Answer:** Refer to response to question #22 for additional information. The goal is to move applications as seamlessly as possible. Initially, the contractor shall discover/gather customer application requirements/characters. Upon gathering customer application requirements/characteristics, the contractor shall make an initial determination as to how seamlessly the customer application(s) will transition to and operate within NITC infrastructure. Transitioning the customer application(s) to NITC infrastructure for testing will allow all parties to determine where changes are required (NITC infrastructure or customer application). Any required customer application modifications resulting from testing can be performed by the customer, or NITC can provide professional services from other specialized subject matter expertise areas to assist. Customer application coding is not a PWS CLIN 025 requirement.*

59. CLINs 1-12. The Performance Standards list Inspection Methods of “Checklist and Customer Input.” Who creates the Inspection Checklists – NITC or the contractor?

    ***Answer**: The inspection checklists are Government created and maintained documents.*

60. Pricing Template. Line 34 “CAF” Column B for the Transition Period show a calculation of 0.75%. Columns C – G provide a Plug number of $100,000. Please clarify that the CAF during the performance period is 0.75% and capped at $100,000 per year?

    ***Answer**: Correct.*

61. PWS Attachment C. The government has provided a sample level of effort with labor hours and estimated FTEs. Request the Government provide metrics for the following:

    a) Number of Servers.

       Answer: 4,152.

    b) Total Number of Security Devices (Firewalls, IDS, ETC).

       Answer: 61.

    c) Total TB of Storage and Storage Type (SAN, NAS, Other).

       Answer: Approximately 1500 PB (15046 TB = SAN - 1742 TB; NAS - 736 TB; Mainframe DASD - 59 TB; Virtual Tape - 456 TB; Open Systems Tape - 11817 TB, Backup Disk Target – 936 TB).

    d) Total Number of Network Devices (Routers, Switches, Telco Devices).

       Answer: 524.

    e) Number of Network Domains to be managed.

       Answer: 1,817 DNS zones managed.

62. RFP Various Attachments. Please provide any documentation that defines the separate and distinct definitions of the different categories of USDA data and information the contractor will be responsible for handling?

    Answer: The question doesn’t provide a sufficient level of detail regarding the terminology “categories” to enable the Government to prepare a response.

63. On page #7 of the RFP, point 2, c, ii, the RFP states that we must provide the resumes for all key positions. While contacting the current key personnel, we have found out that the incumbent has **bind** current key personnel to exclusive agreements. This gives a **very large unfair** advantage to incumbent since any non-incumbent firm will have to propose key personnel not on the contract.

    a) Since the incumbent has forbidden the current contract employees from sharing their resumes,

       i. Will government consider removing the requirement of all resumes except program manager? Or
       ii. Could we provide the information requested such as education, certification, experience, background investigation status and special skills in lieu of their resumes?

       ***Answer**: The resume requirements remain unchanged.*

b) We have the ability to propose an entirely new team on contract. Would government rate incumbent employees resume for key personnel higher than resume with all skills and equal or more number of year of experience but without NITSI experience?

***Answer*: The evaluation will be conducted in accordance with the RFP.**

c) At this time, we see no way for a fair and reasonable competition to occur and any instance of JMA-IT being favorably rated for having current personnel would mean that they truly had blocked out competition, which is not allowed under the FAR. Is the Government going to direct the incumbent to remove the exclusive and unethical agreements (Which are typically ruled illegal) and inform their staff that they are free to pursue options as they see fit?

***Answer*: No. The Government will have no communication with the incumbent contractor regarding the subject acquisition**.

64. On page 10 of the RFP, point 8.5, it is stated that the labor hours expended must be included on the invoice? Is this needed for team members who are working on the FFP CLINs? Is this information needed for purely informational purposes?

    ***Answer*: Yes. The labor hours expenditure information/documentation is required for all FFP CLINs and LH CLINs. The information/documentation for the FFP CLINs is required to support internal accounting classification requirements associated with NITC's client billings and service offerings.**

65. On page 10 of the RFP, point 8.5, there does not seem to be instructions regarding the invoicing FFP CLINs. Could you provide instructions addressing matters regarding invoicing FFP CLINS, such as how much should be billed monthly? Should the amount be the FFP divided by 12? Should be amount be equivalent to a daily charge multiplied by the number of business days in the month?

    ***Answer*: The amount to be included on the monthly invoices for the FFP CLINs shall be calculated as 1/12 of the annual price.**

66. On page 10 of the RFP, point 8.5, there does not seem to be instructions regarding the invoicing FFP CLINs. Should time off during the month by the FFP employee affect the monthly invoiced amount?

    ***Answer*: No. Refer to the response to question #65. The annual FFP shall be built with the consideration of factors such as time off, training, etc.**

67. Could you provide a sample Monthly Status Report as an attachment to the PWS, just as you did with Attachment E, for informational purposes?

    ***Answer*: No. The contractor will be responsible for the development of the report.**

68. Could you provide a sample Scheduled Absence Calendar Availability deliverable as an attachment to the PWS, just as you did with Attachment E, for informational purposes?

    ***Answer*: No. The contractor will be responsible for the development of the deliverable.**

69. In the performance standards/acceptable quality levels/incentive/disincentive section for the FFP CLINs, there are payment reductions of a certain percentage. For example, on CLIN 001 the "Continuous Assessment Tasks" performance requirement shows a 1% payment reduction up to the maximum of $2500. How will these % reductions be calculated? Will this be a % of the total invoice for the month? Will this be a % of the billed amount for all the work on this CLIN? Since the Acceptable Quality Level is at the overall CLIN level, we assume these penalties cannot be calculated as a % of the billable amount for a particular individual working on this CLIN in a particular month, correct?

Answer: ***The disincentive amount (i.e. payment reduction) will be calculated based on the total monthly CLIN price.***

70. In the CLIN 001 performance standards description, performance requirement "A-123," the documentation states that there will be a payment reduction of 1 % for grammar errors. How will grammar be judged and how will disputes regarding proper be arbitrated?

    Answer: ***Refer to the response to question #33 regarding applicable grammatical standards. In the event that a violation is identified, the contractor will be notified of such violation and be provided the opportunity to respond accordingly. The Contracting Officer possesses the final authority to determine if the application of a payment reduction(s) is warranted.***

71. In the CLIN 001 performance standards description, performance requirement "Weekly Status Report," the document states that there will be a 3% payment reduction for two or more violations. Does this mean that 2 or more grammatical errors in any of the 12 Weekly Status Reports will result in a 3% payment reduction? We assume a Weekly Status Report is require for each team member working on this CLIN. This question applies to most of the FFP CLIN descriptions.

    Answer: ***The weekly report is required for the CLIN, not the individuals supporting the CLIN. If there are four weekly reports due during a given monthly reporting period, a payment reduction may be warranted after the confirmed identification of a second violation.***

72. On the description for CLIN 009, under performance requirement "Personnel Availability," is the AQL sentence "No more violation per month," complete, or is this a word missing?

    Answer: ***Please note that the correct reference should be "CLIN 010" (refer to the response to question #24 for details). The CLIN 010 document has been further updated.***

73. On the description for CLIN 009, under performance requirement "Personnel Retention," does this 10% calculation include contract employees who leave us to become federal employees at the USDA?

    Answer: ***Yes; however, please note that the correct reference should be "CLIN 010".***

74. On attachment C, what is the purpose of the CLINs with zero FTE estimated?

    Answer: ***Column D of PWS Attachment C identifies the estimated number of FTE positions that may be required at commencement of the task order. As such, the identification of the number zero indicates that there may not be a need for support at the commencement of the task order; however, it is anticipated that support may be required during the life cycle of the task order, thus, such CLINs have been included to ensure maximum availability and flexibility to support future needs.***

75. Since the Task Order Manager role is estimated at 2 FTE in attachment C and the CLIN description for the Task Order Manager says there is to be one TOM who is responsible….. Do we need to adjust the FTE allocation on the CLINs which will have team members who will also be performing work on this TOM CLIN. In other words, if we plan to fill part of the second TOM FTE with someone who also works on CLIN 028 should we provide an estimate for CLIN 028 that has only 18.8 FTEs because the other .2 FTE will be allocated to this person's work on CLIN 10?

    Answer: ***It is the contractor's responsibility to develop and propose a staffing plan that is sufficient to perform and complete the stated requirements. Refer to the response to question #14 for further information and details.***

76. On attachment C, the Task Order Management CLIN is shown as CLIN 10, though the title at the top of the Task Order Management CLIN description document lists CLIN 009. Does one of these CLIN designations need to be changed, so that the TOM CLIN number is the same in both places?

    ***Answer:* Refer to the response to question #24.**

77. On CLIN 23, 24, 27, and 28, what are the different skill levels required? According to Attachment C, NITC does want different skill levels, though there is no additional information in the CLIN description document to tell what different skill levels are wanted as there was for other CLINs such as CLIN 20.

    ***Answer:* It is the contractor's responsibility to develop and propose a staffing plan that is sufficient to perform and complete the stated requirements. No additional information will be provided. The Government has indicated that it may be possible to complete the task requirements for such CLINs via the utilization of varying skill levels; however, it is ultimately the contractor's responsibility to develop and propose a staffing plan that the Government will evaluate in accordance with the RFP.**

78. What does "Estimated Core FTEs" mean In attachment C column "D". Are the "Estimated Core FTEs" supposed to represent the Government's estimate on the maximum amount of FTEs per CLIN or their estimated keys per CLIN or something else?

    ***Answer:* Refer to the responses to questions #14 and #75.**

79. For calculating the price, is the Government basing it's evaluation on 96 FTEs as identified in attachment C, or is it based on a set number of hours, or is it up to the offeror to propose the their estimate based on the solicitation documentation with 96 FTEs as a guideline? The concern is that most of the CLINs are T&M and a LH contract can be bid at less FTEs and government will end up paying later on more based on actual LH. Also there is no workload provided to estimate the level of effort. We recommend government to enforce pricing to be based on fix number of hours so that government can compare Apple to Apple.

    ***Answer:* Refer to the response to question #14. The total evaluated price/cost will be obtained from the pricing template. As per paragraph (V)(B)(3) of the RFP, the price will be evaluated for realism.**

80. Can the Cover Letter, a table of contents, and acronym list be excluded from the 45 page maximum page count described on page 5 of the RFP section, "IV. Proposal Content"?

    ***Answer:* No; however, the standalone file containing the cover letter (reference RFP paragraph (III)(A)(3)) is excluded from the page limitation.**

81. Can key resumes be excluded from the 45 page maximum page count described on page 5 of the RFP section, "IV. Proposal Content and provided as a separate attachment?

    ***Answer:* No.**

82. Is the Government expecting offerors to provide a technical approach writeup for each of the 29 CLINs?

    ***Answer:* Refer to the response to question #17.**

83. Do CLINs cross multiple divisions of the CIO? If so please advise on which.

    Answer: CLIN 028, System Administration Services, is currently the only CLIN that supports multiple divisions within NITC. CLIN 028 supports IOD/SNCC (current staffing level is

approximately 1 FTE); SED/OSB (current staffing level is approximately 12 FTE); and SED/WSB (current staffing level is approximately 6 FTE).

Refer to "Clarification Document – Attachment G" for information pertaining to the organizational structure.

84. RFP, III.A.1, Submission of Proposal, page 4. Offerors are instructed to deliver hard copies of our proposals within 24 hours following the close date/time, which is Saturday, January 31, at 5 p.m. Will a Government representative be available to receive proposals? Alternately, would the Government consider accepting hard copy proposals on or after Monday, February 2?

    Answer: Refer to the response to question #35.

85. RFP, III.A.1, Submission of Proposal, page 4. In regard to the hard copy submittals, should offerors include Factors 1, 2, and 3 in the same notebook?

    Answer: The hard copy submittal shall be consistent with the electronic submission as per the instructions in RFP paragraph (III)(A)(3).

86. RFP, III.A.1, Submission of Proposal, page 4. If using 11 x 17-in. paper for the organization chart, will this page count as a single page?

    Answer: Yes.

87. RFP, III.A.1, Submission of Proposal, page 4. Would the Government consider allowing offerors to use a font size smaller than 11 pt Times New Roman in graphics, tables, charts, etc. provided the text is legible?

    Answer: No.

88. RFP, III.A.1, Submission of Proposal, page 4. Would it be acceptable to include page nos., RFP no., and other identifying information in the headers and footers in a smaller font and outside of the 1-inch margin?

    Answer: Yes.

89. RFP, IV.B.1, Cover Letter, page 5. Is the cover letter included in the 45-page limit for overall proposal content?

    Answer: No. The standalone file containing the cover letter is excluded from the page limitation.

90. RFP, IV., Proposal content. Should offerors include a cover, title page, table of contents, and, for the hard copies, tabs? Will these be included in the 45-page limit?

    Answer: The contractor submission shall comply with the requirements set forth in the RFP. The standalone file containing the cover letter is excluded from the established page limitation. All other documentation is included within the established page limitation. Tab separators with no written content are not included within the established page limitation.

91. RFP, IV.B.2.b, Quality Control Plan (QCP), page 6. Would the government consider taking the QCP outside of the 45-page limitation and allow delivery in an appendix?

    Answer: No.

92. RFP, IV.B.2.a.ii and IV.B.2.c, Implementation (and referenced PWS 8.7.1 Phase-In Plan) Staffing Approach/Plan, page 10 and 6. Section IV.B.2.a.ii requires the identification of resources required to complete transition related tasks during the transition period. PWS section 8.7.1, first bullet, calls for a staffing plan to be provided. Section IV.B.2.c requires a staffing plan for the entire program. Can

the government confirm that the resource / staffing plan in Section IV.B.2.a.ii and PWS 8.7.1 is specific to transition only, and is different from the Staffing Plan is Section IV.B.2.c?

***<u>Answer</u>*: It is confirmed that the requirements identified in RFP paragraph (IV)(B)(2)(a)(ii) and PWS paragraph 8.7.1 are specific to transition period and phase-in requirements as identified within the referenced documents. It is the contractor's responsibility to develop and propose a staffing plan that is sufficient to perform and complete the stated requirements, inclusive of phase-in requirements.**

93. RFP, IV .B.2.c.ii, Resumes, page 7. Are resumes included in the 45-page limit or can they be placed in an appendix that is excluded from the page limit?

    ***<u>Answer</u>*: Yes, resumes are included within the established page limitation. If submissions include appendices, such appendices will be included within the established page limitation.**

94. RFP, IV .B.2.c.ii, Resumes, page 7. Does the Government have a preferred format for the resumes? Will the government provide the page limitation for each resume?

    ***<u>Answer</u>*: No, there is not a preferred format for resumes. No, the Government will not establish a page limitation for each resume.**

95. RFP, IV.B.4, Price Submission, page 9. Please confirm that the five pages that are allowed for the Price Submission (and that exclude Attachment 2) are excluded from the 45-page limit.

    ***<u>Answer</u>*: Confirmed. As per RFP paragraph (IV)(A)(3) the price submission is not included within the established page limitation.**

96. RFP, IV.B.3.b, Past Experience and Performance, page 8. If a member of a JV has a past performance that is more relevant with regard to size, scope, and complexity than a JV performed past performance, can member past performance be used to address the $2 million annual revenue requirement without being non-compliant and without penalty?

    ***<u>Answer</u>*: The submission shall comply with the following requirement as per RFP paragraph (IV)(B)(3)(b): "<u>If the ASB prime contractor is a Joint Venture (JV) company that has no relevant past/present performance, which shall be clearly stated within the proposal</u>, then the Government may consider one reference from one partner of the JV to meet the requirement in the preceding sentence regarding minimum performance requirements as a prime contractor." It is the ASB prime contractor's responsibility to render a determination confirming that the JV does NOT have relevant past/present performance. Such determination shall be documented within the proposal submission.**

97. CLIN 029, section 2.a, Scope/Duties, page 1. Re: Install, operate and maintain HP OpenView applications in an enterprise environment, including the Business Availability Center, HP OpenView agents, and the Business Process Monitor components -- Is this software currently in use at NITC? If so, what is meant by the requirement to "Install"? If not, what software is currently being utilized to monitor NITC systems?

    Answer: All software is currently installed and in use. From time to time, the requirement to perform a complete "install" (i.e. from scratch) will be deemed necessary (expansion, major software upgrades, etc.).

98. CLIN 029, section 2.b, Scope/Duties, page 1. Re: Install, operate and maintain the XYMON monitoring application in an enterprise environment -- Is this software currently in use at NITC? If so, what is meant by the requirement to "Install"? If not, what software is currently being utilized to monitor NITC systems?

Answer: All software is currently installed and in use. From time to time, the requirement to perform a complete "install" (i.e. from scratch) will be deemed necessary (expansion, major software upgrades, etc.).

99. CLIN 029, section 2.c, Scope/Duties, page 1. Re: Install, operate and maintain Microsoft's System Center Operation Manger (SCOM) application in an enterprise environment -- Is this software currently in use at NITC? If so, what is meant by the requirement to "Install"? If not, what software is currently being utilized to monitor NITC systems?

    Answer: The reference to "SCOM" is not included within the referenced location; however, it is located in section 2.d. All software is currently installed and in use. From time to time, the requirement to perform a complete "install" (i.e. from scratch) will be deemed necessary (expansion, major software upgrades, etc.).

100. CLIN 029, section 2.d, Scope/Duties, page 1. Re: Install, operate and maintain Microsoft's System Center Operation Manger (SCOM) application in an enterprise environment. -- Is this software currently in use at NITC? If so, what is meant by the requirement to "Install"? If not, what software is currently being utilized to monitor NITC systems?

    Answer: All software is currently installed and in use. From time to time, the requirement to perform a complete "install" (i.e. from scratch) will be deemed necessary (expansion, major software upgrades, etc.).

101. CLIN 029, section 2.m, Scope/Duties, page 1. Re: Document changes, incidents, and problems using NITC's Configuration Management Tools and Systems. -- What system, if any, is currently being utilized to track NITC Incidents, Problems and Change Requests?

    Answer: BMC Remedy ITSM Suite.

102. CLIN 028, section 2.d, Scope/Duties, page 1. Re: Install, test, configure, customize, and maintain various server operating systems and associated software utilizing physical and virtual hardware. Utilize automated provisioning techniques to deploy new systems and software -- Does NITC utilize imaging software for the deployment of servers? If so, what imaging software is used?

    Answer: For virtual Windows and RedHat Linux systems, the OSB-VMware team utilizes VMWare Templates and where applicable VMware vCAC to do automated builds off of OS templates that OSB Linux/WSB maintain. This is an automated process and is well thought out and working today. The Linux team in addition utilizes scripting techniques to maintain hardened/patched systems immediately after build.

    Physical Windows systems images are maintained images of operating systems within BMC's BladeLogic Server Automation product. These golden-images are copies of the operating systems which are maintained independently with the necessary security configurations, hardening templates, patch updates as well as vulnerability mitigations.

    Physical RedHat Linux systems utilize kickstart for building systems according to a well maintained set of build scripts that are also utilized in part of the process for creating RedHat Linux virtual systems from the template process mentioned above.

    Solaris Virtual and Physical machines are built utilizing JumpStart and Image Packaging System/Automated Installer for Solaris 10/11 builds respectively. Configuration settings and hardening are applied with those products using well-maintained scripts.

    AIX virtual and physical machines are deployed utilizing NIM and well maintained mksysb images (golden images).

103. CLIN 028, section 2.h, Scope/Duties, page 1. Re: Perform patch/fix research and operating system software upgrades through service packs and other software bundling methodologies. The contractor

shall use current NITC patching techniques and automated patching products used at the NITC -- What patching software is currently in use at NITC?

Answer: Within one Windows environment, Tivoli Endpoint Manager (TEM) is used as the centers patching solution. In another environment, Windows Server Update Services (WSUS) provides the needed patches and BladeLogic Server Automation (BSA) provides the "intelligence" behind the installation of those patches.

All Linux patching is done utilizing RedHat Satellite and BMC Server Automation patching techniques. Solaris patching is accomplished through manual application of Critical Patch Updates from Oracle. AIX patching is accomplished through manual application of IBM service packs.

104. CLIN 028, section 2.i, Scope/Duties, page 1. Re: Utilize volume management techniques to create, maintain, expand, and shrink file systems; monitor performance of the file systems; and utilize RAID techniques and practices for availability and performance -- How much storage is currently in use at NITC and what, if any, software tools are being utilized to manage that storage environment?

Answer: NITC manages approximately 1500 petabyte (PB) plus of storage. Hitachi Storage Navigator and HiCommand are used to manage SAN storage arrays. NetApp OpsManager is used to manage NAS storage. Enterprise Manager is used to manage EMC storage. NetBackup OpsCenter is used to manage backups. APTARE software is also utilized for gathering reports. Management consoles are used on NetApp, EMC, NetBackup, and Hitachi. These tools are used by the storage administrator.

105. CLIN 023, section 2.a, Scope/Duties, page 1. Re: Installs, administers and manages the NITC Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS), Security Incident and Event Manager (SIEM), Wireless Intrusion Prevention Systems (WIPS) and Host-based Intrusion Detection systems (HIDS/HIPS) -- What software tool does NITC use to administer their security?

Answer: IDS/IPS – Sourcefire; SIEM - Mcafee ESM; and WIPS – Motorola AirDefense.

106. CLIN 002, section 1, Overview, page 1. Does the role of Budget Analysis present an Organizational Conflict of Interest for the winning contractor in any future bids for Government organizations using NITC?

Answer: No.

107. CLIN 002, section 1, Overview, page 1. Does the role of Budget Analysis currently exist and does it place the incumbent in an OCI situation?

Answer: Yes, the position currently exists. There is no OCI with the current support being provided.

108. CLIN 003, section 1, Overview, page 1. Re: The objective is to obtain services to support the NITC Business Continuity Program. The contractor shall develop IT disaster recovery (DR) and continuity of operations (COOP) plans and test schedules and shall coordinate and conduct COOP and DR tests Do the DR, and COOP plan currently exist and need to be updated, or are these plans to be developed by the winning contractor?

Answer: The plans already exist and shall be updated as required.

109. CLIN 006, section 1, Overview, page 1. Can the Government clarify the role and its relation to the A&A process? Is this role supporting the A&A efforts, or performing those efforts?

Answer: The contractor will be directly responsible for performing the Continuous Assessment & Authorization tasks consistent with the USDA's Risk Management Framework (Steps 1-3) and the scope of work detailed in CLIN 006.

110. CLIN 007, section 4, Performance Standards/Acceptable Quality Levels/Incentive/Disincentive, page 4. Re: 100% of all ITSM Process and Development and Documentation activities shall be conducted in accordance with governmental & organizational standards, policies, directives, standard operating procedures, work instructions, processes & guidance. All operational support activities shall be captured and properly documented in the organizational ITSM tool. The contractor shall adhere to this requirement unless a written exemption is issued by an authorized Government representative--This performance standard covers all activities on the contract. For example, if a System Administrator violates the Change Management policy that would violate this Performance Standard. Question: Can the Government re-write this standard to address strictly the performance of the duties of this position, not all activities conducted in regard to all ITSM processes?

Answer: No.

111. CLIN 011, section 2.t, Scope/Duties, page 2. Re: Creation of Virtual Desktop Infrastructure (VDI) designs and its implementation and documentation--Does NITC currently possess a VDI environment, if so what software tools are utilized to produce and maintain this environment?

Answer: NITC currently supports assorted Citrix environments.

112. CLIN 012, section 4, Performance Standards/Acceptable, page 2. CLIN 012 contains 3 performance standards, yet RFP Attachment 1 - PWS Attachment C Quality Levels/Incentive/Disincentive and Excel spreadsheet allocates no FTE to perform the actions to meet the performance standard. How is the contractor to be held to performance standards with no staff to perform?

Answer: Refer to the response to questions #34 and #74. Furthermore, refer to paragraph (IV)(B)(4) of the RFP regarding the Government's right to award the support for each CLIN on an individual basis.

113. CLIN 013, section 1, Overview, page 1. Re: The contractor shall provide BMC Software Atrium Discovery and Dependency Mapping (ADDM) system administration and application modeling services for the support and management of the ADDM software product and supporting infrastructure -- as ADDM is a tool utilized for Service Asset and Configuration Management in the Remedy tool suite -- Will the Government provide a clear delineation between the activities performed in CLIN 0008 and those performed here in CLIN 13?

Answer: The CLINs are clearly distinguishable from each other. CLIN 008 is for a Process Specialist Support role that acts as a consumer and user of the BMC Remedy ITSM Suite; this position is not deemed System Admin Technical in any manner. CLIN 008 performs configuration management database (CMDB) data entry, manipulation, and quality assurance tasks, etc. CLIN 013 requires subject matter expertise be provided to support the requirements identified within the CLIN. CLIN 013 performs ADDM administration and application modeling tasks, etc.

114. CLIN 014, section, 2.i, Scope/Duties, page 1. Re: Examples of COTS packages currently supported: § Web Application Servers: WebSphere, WebLogic, Tomcat, JBoss, Apache § Content Management: Oracle WebCenter Content, Drupal, Alfresco § Portal: WebSphere Portal § Business Intelligence: Oracle EPM, Oracle OBIEE, IBM Cognos § Search Tools: Google Search Appliance § Social Media Tools: IBM Lotus Connections § Other: IBM Tivoli Usage and Account Manager, BMC Remedy, HP LoadRunner – Is the list of "example COTS packages" all inclusive? If not please provide an exhaustive list.

Answer: As stated in the PWS, the list provided represents a sampling of the COTS products in use and can change based on customer requirements.

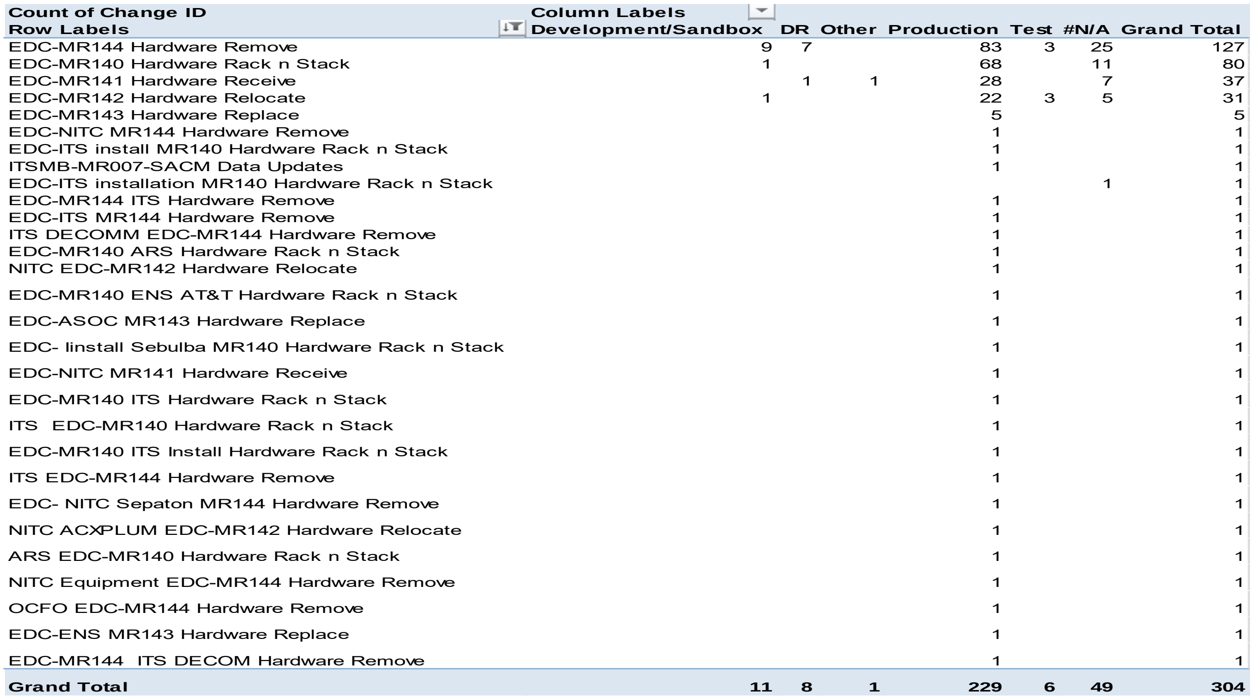
115. CLIN 015, section 2.a, Scope/Duties, page 1. Re: Determine, identify and coordinate electrical power requirements for new and existing IT hardware in the NITC Enterprise Data Center. To allow the

proper sizing of the FTE requirement, would the government please provide the monthly number of adds, changes, and deletes of hardware to the infrastructure by type?

Answer: The estimated number of power related changes is 17. The count does not include Incident tickets and service requests.

116. CLIN 015, section 2.b, Scope/Duties, page 1. Re: Coordinate IT hardware placement, installation, move, replacement, and removal activities. -- To allow the proper sizing of the FTE requirement, would the government please provide the monthly number of adds, changes, and deletes of hardware to the infrastructure by type?

Answer: The image below reflects an estimate of the identified activities. The count does not include Incident tickets and service requests.



Count of Change ID	Column Labels						
Row Labels	Development/Sandbox	DR	Other	Production	Test	#N/A	Grand Total
EDC-MR144 Hardware Remove	9	7		83	3	25	127
EDC-MR140 Hardware Rack n Stack	1			68		11	80
EDC-MR141 Hardware Receive		1	1	28		7	37
EDC-MR142 Hardware Relocate	1			22	3	5	31
EDC-MR143 Hardware Replace				5			5
EDC-NITC MR144 Hardware Remove				1			1
EDC-ITS install MR140 Hardware Rack n Stack				1			1
ITSMB-MR007-SACM Data Updates				1			1
EDC-ITS installation MR140 Hardware Rack n Stack						1	1
EDC-MR144 ITS Hardware Remove				1			1
EDC-ITS MR144 Hardware Remove				1			1
ITS DECOMM EDC-MR144 Hardware Remove				1			1
EDC-MR140 ARS Hardware Rack n Stack				1			1
NITC EDC-MR142 Hardware Relocate				1			1
EDC-MR140 ENS AT&T Hardware Rack n Stack				1			1
EDC-ASOC MR143 Hardware Replace				1			1
EDC- Iinstall Sebulba MR140 Hardware Rack n Stack				1			1
EDC-NITC MR141 Hardware Receive				1			1
EDC-MR140 ITS Hardware Rack n Stack				1			1
ITS EDC-MR140 Hardware Rack n Stack				1			1
EDC-MR140 ITS Install Hardware Rack n Stack				1			1
ITS EDC-MR144 Hardware Remove				1			1
EDC- NITC Sepaton MR144 Hardware Remove				1			1
NITC ACXPLUM EDC-MR142 Hardware Relocate				1			1
ARS EDC-MR140 Hardware Rack n Stack				1			1
NITC Equipment EDC-MR144 Hardware Remove				1			1
OCFO EDC-MR144 Hardware Remove				1			1
EDC-ENS MR143 Hardware Replace				1			1
EDC-MR144 ITS DECOM Hardware Remove				1			1
Grand Total	**11**	**8**	**1**	**229**	**6**	**49**	**304**

117. CLIN 016, section 2, Scope/Duties, page 1. Re: The contractor shall provide systems database administration support - To allow the proper sizing of the FTE requirement, would the government please provide the number of, and size of the databases to be supported by type (e.g. Oracle, SQL, DB2, etc.)?

Answer: The number of databases are identified by type: Adabas (25); DB2 (245); IDMS (20); MySQL (65); Oracle (167); SQL Server (256). The sizes vary in range from 1GB to 12TB.

118. CLIN 016, section 2, Scope/Duties, page 1. Re: The contractor shall provide systems database administration support -- To allow the proper sizing of the FTE requirement, would the government please provide the number (on a monthly basis) of the databases change requests to be supported by type (e.g. Oracle, SQL, DB2, etc.)?

Answer: Change requests vary per month based on customer requirements and range from single to double digits per month. Average database changes by type are as follows: Adabas (5); DB2 (10); IDMS (2); MySQL (4); Oracle (11); SQL Server (2). The average counts do not include Incident tickets and service requests.

119. CLIN 027, section 1, Overview, page 1. In order to determine the number of FTE required to perform this function, would the government please provide the number of Storage devices, LUNs, size of each LUN and the number of change requests on a monthly basis?

Answer:* *The number of storage devices is 853 (Disk Device, Tape Drives, Libraries and Servers). The number of LUNs is 50,000. The LUN sizes vary from 1GB to upwards of over 3200GB, with many different sizes in between. Custom volumes are also created and maintained. The average number of change requests per month is 12, which does not include incident tickets and service requests.

120. CLIN 028, section 1, Overview, page 1. In order to determine the number of FTE required to perform this function, would the government please provide the number of systems, by Operating System and Virtual as well as Iron?

Answer: The table below reflects the requested information.

Row Labels	**Server (AIX)**	**Server (Linux)**	**Server (Solaris)**	**Server (Windows)**	**Grand Total**
Managed Hosting	**5**	**689**	**152**	**1171**	**2017**
Physical	1	441	100	303	845
Virtual	4	248	52	868	1172
PaaS	**32**	**910**	**144**	**1049**	**2135**
Physical		1			1
Virtual	32	909	144	1049	2134
Grand Total	**37**	**1599**	**296**	**2220**	**4152**

121. RFP Attachment 1 – PWS, section 4, Applicable Documents, page 6. The link in bullet 1 (http://wiki.edc.usda.gov/mediawiki/index.php/Main_Page) is non-responsive Can USDA please provide access so we may review?

Answer:* *Refer to the response to question #56.

122. RFP Attachment 1 – PWS, section 7.1, Quality Control, page 8. Paragraph 1 references 'the applicable Inspections of Services Clause.' Can USDA please provide that clause or tell us what that clause references?

Answer:* *FAR 52.212-4, Contract Terms and Conditions – Commercial Items (Dec 2014), Alternate I (May 2014).

123. RFP Attachment 1 – PWS, section 8.7.1, Phase-In Plan, plan 11. Bullet number 2 in this section requires the inclusion of our plan for "Development and submission of required deliverables." These deliverables are not identified in the PWS. Could the government define what the minimum required deliverables are for the Phase In Plan?

Answer:* *The referenced bullet is for contractor proposed deliverables.

124. Specification, CLIN 001 & CLIN 006, Audit Support Info Sys Security Supt. Hyperlinks included in each specification are non-responsive: ("Appendix E - Security Controls Assessment List" and "USDA Six Step Risk Management Framework Process (RMF) Guide") Can USDA please provide access so we may review?

Answer: Refer to "Clarification Document – Attachment A" and "Clarification Document – Attachment B".

125. PWS/CLINs, CLIN016, Database Administration Services. Request additional information regarding CLIN016. Specifically:

a) Total number of DB instances.

Answer: Over 700 database instances.

b) Approx. number of databases.

Answer: Approximately 700 databases.

c) Breakdown of instances by RDBMS PWS/CLINs.

Answer: Adabas (25); DB2 (245); IDMS (20); MySQL (65); Oracle (167); SQL Server (256).

126. CLIN018, Network Engineering Services. Request additional information regarding CLIN018. Specifically:

a) Number of routers and switches.

Answer: Number of routers is 255. Number of switches is 269.

b) Number of routers and switches by location PWS/CLINs.

Answer: KC (298); STL (117); DC (85); FTC (12); FTW (4); SLC (8).

127. CLIN025, Senior Application Engineering Services. Request additional information regarding CLIN025. Specifically:

a) Number of Major and Minor Apps hosted.

Answer: The number of major (those applications that require large databases and other application interdependencies) and minor (e.g., small WEB applications) vary. For customer/agency-wide application transitions, NITC has transitioned as many as approximately 100 applications.

b) Rough breakdown of app hosting platforms by OS.

Answer: Refer to "Clarification Document – Attachment C" and "Clarification Document – Attachment D".

c) Load balancer manufacturer PWS/CLINs.

Answer: NITC primarily utilizes F5 load balancers, but also supports Cisco CSS, CSM and ACE load balancers.

128. CLIN027, Storage Administration Services. Request additional information regarding CLIN027. Specifically:

a) Number of enterprise disk arrays.

Answer: The number of enterprise disk arrays is as follows: HDS (6), EMC (4), and NetApp (14).

b) Total storage capacity.

Answer: Total storage capacity is 1500PB.

c) Breakdown of arrays by vendor.

Answer: Refer to the answer to question 128(a).

d) Annual storage growth estimate.

Answer: The annual storage growth estimate is 20%.

In addition to the information provided above, there are over 200 CIFS and NFS volumes.

129. PWS/CLINs, CLIN028 Systems Administration Service. Request additional information regarding CLIN028. Specifically:

a) Total number of servers.

Answer: Refer to the response to question #120.

b) Number of servers by OS.

Answer: Refer to the response to question #120.

c) Numbers of prod vs. test.

Answer: The table below reflects the requested information.

Row Labels	**Server (AIX)**	**Server (Linux)**	**Server (Solaris)**	**Server (Windows)**	**Grand Total**
Managed Hosting	**5**	**689**	**152**	**1171**	**2017**
Physical	**1**	**441**	**100**	**303**	**845**
Acceptance		15	15	7	37
Development/Sandbox		57	9	32	98
DR		72	5	32	109
Other		1	1		2
Production	1	290	53	221	565
Test		6	17	9	32
(blank)				2	2
Virtual	**4**	**248**	**52**	**868**	**1172**
Acceptance		29	5	70	104
Development/Sandbox		51	16	242	309
DR		52	1	141	194
Production	4	104	22	388	518
Test		12	8	27	47
PaaS	**32**	**910**	**144**	**1049**	**2135**
Physical		**1**			**1**
Acceptance		1			1
Virtual	**32**	**909**	**144**	**1049**	**2134**
Acceptance		191	10	157	358
Development/Sandbox	3	222	46	204	475
DR	4	8	2	5	19
Production	10	432	74	585	1101
Test	15	56	11	95	177
(blank)			1	3	4
Grand Total	**37**	**1599**	**296**	**2220**	**4152**

d) Percentage of servers that are virtualized.

Answer: Refer to the response to question #120.

130. RFP IV.B.1. Will the Government confirm that the 2 page cover letter is not subject to the overall 45 page limit?

***Answer:* Yes. The standalone file containing the cover letter is excluded from the page limitation.**

131. RFP IV.B. Can offerors submit a 2 page executive summary, not to be subject to the overall 45 page limit?

***Answer:* No. Such documentation would be subject to the established page limitation.**

132. RFP IV.B.2.c.ii. Will the Government confirm that resumes for Key Personnel are not subject to the overall 45 page limit?

***Answer:* No. The resumes are subject to the established page limitation.**

133. RFP IV.B.3. Will the Government confirm that the 2 page Past Experience and Performance references are not subject to the overall 45 page limit? Additionally, with 2 pages per citation and 29 task areas, the Offeror will have approximately 3 typed lines (equivalent to 1-2 sentences) to describe their similar experience. To ensure adequate detail, will the Government considering allowing the offeror a minimum of 4 pages per reference?

***Answer:* No. The past experience and performance references are subject to the established page limitation. The specific page limitation for past experience and performance reference information remains unchanged.**

134. RFP IX. The RFP states, "Electronic proposals must be submitted no later than the date established in the eBuy, with six hardcopies to be delivered within 24 hours of this date/time…" eBuy provides the due date of Friday, 1/30. In our experience, deliveries attempted on the following day (Saturday, 1/31) may not be accepted by building security. Would the Government please consider changing the 24 hour timeframe for hardcopy delivery to 1 business day, making the due date Monday, 2/2?

***Answer:* Refer to the response to question #35.**

135. RFP IV.B. For ease of evaluation, will the Government confirm that offerors may submit a Cross Reference matrix demonstrating compliance with the RFP, not to be subject to the overall 45 page limit?

***Answer:* No. Such documentation would be subject to the established page limitation.**

136. RFP IV.B.2, PWS 5. The RFP states, "The proposal shall include sufficient documentation to demonstrate both a detailed understanding of the stated requirements and the potential management challenges associated with the broad range of task areas involved." In order for offerors to address the requirements and management challenges for all 29 task areas, will the Government consider expanding the overall page limit to 60 pages?

***Answer:* No.**

137. PWS Attachment C, Column D. Are the Estimated Core FTEs (QTY 96) mandatory?

***Answer:* Refer to the response to question #14.**

138. RFP Attachment 2, Tab labeled "Totals". Pricing Template - can you change the growth factor percentage formula in Fields C38, C39, D38, D39, E38, E39, F38, F39, G38, G39?

***Answer:* No.**

139. Page 4, RFP IDO5140054, III - Instructions to Contractors. Font type-size - will the government allow the use of different font styles and/or sizes for tables and graphics?

***Answer:* No.**

140. Page 4, RFP IDO5140054, III - Instructions to Contractors. Would the government consider excluding resumes and past performance from the overarching response page limitation of 45 pages?

***__Answer__*: No.**

141. RFP IV Proposal Content, B. 1 Cover Letter, page 5. Section B. Detailed, 1. states "this cover letter shall be no more than 2 pages." Question: Is the cover letter's two pages included within the 45-page limit for the technical proposal (RFP IV. 3) or is the cover letter in addition to that 45-page limit?

***__Answer__*: Yes. The standalone file containing the cover letter is excluded from the page limitation.**

142. RFP IV Proposal Content, B 2. Technical Approach b) Quality Control Plan page 6. Does the government have a Quality Assurance Surveillance Plan (QASP) already in place that will govern the contractor's Quality Control Plan (QCP)? If so, please provide the QASP, as part of the materials in this solicitation.

***__Answer__*: No, there is not an existing Government developed QASP that will govern the contractor's QCP. The Government's QASP will not govern the contractor's QCP.**

143. Attachment 3 Past Performance Questionnaire, page 1. Please confirm the number of questionnaires to be submitted for each past performance reference. Page 1 of Attachment 3 has a table that indicates Contracting POC and Technical POC. Should separate questionnaires be submitted from the Contracting POC (COR) and the Technical POC (COTR) to GSA.

***__Answer__*: One questionnaire shall be submitted for each past performance reference.**

144. RFP IV Proposal Content, 3. Page 5. RFP IV. 3. states "Each proposal shall be….. no smaller than 11 point type-size,…..Question: Will the government exclude text in the organization chart, in tables, and in graphics from this requirement and instead allow no smaller than 8 point type-size?

***__Answer__*: No.**

145. RFP IV. 3, page 5. The RFP states "Overall proposal content, excluding pricing submission, shall be no more than 45 pages in length."Question: Is the title page (cover), table of contents and list of exhibits excluded from that 45 page count?

***__Answer__*: No; however, the standalone file containing the cover letter is excluded from the page limitation.**

146. The RFP, Page 5, IV.A.3, states that "Each proposal shall be legible, single-spaced, typewritten Times New Roman font (no exceptions) no smaller than 11 point type-size…"

a) Given the volume of content required within the 45-page limit, will the Government consider reducing the font size requirement to less than 11 point for exhibits, figures, and tables?

***__Answer__*: No.**

b) If so, would Arial Narrow 8 for graphics and Arial Narrow 9 for Tables be acceptable?

***__Answer__*: N/A.**

147. The RFP, Page 5, IV.A.3, last sentence states that "Overall proposal content, excluding the pricing submission, shall be no more than 45 pages in length."

a) May the cover page, Table of Contents, and 2-page Cover Letter be EXCLUDED from the page count.

***__Answer__*: Request partially denied. As per the RFP, said information, with the exception of the standalone cover letter document/file, shall be included within the established page limitation.**

b) In order to maximize our description of our Technical Solution and Staffing, may we EXCLUDE the following from the 45-page limit
   - The detailed Resumes required for all Key Personnel, page 7, Section IV, B.2.c.ii, of the RFP
   - The 3 Past Performance reference descriptions (max. of 2 pages each) required on page 8, Section IV, B.3.b, paragraph 1 of the RFP
   - The Quality Control Plan (required in Section IV, B.2.b page 6 of the RFP)

   Answer*:** ***No.

148. The RFP, page 6, 2.a).i states "The technical proposal shall include a description of how the technical approach (i.e. description of the tasks to be performed) and analytical techniques will be applied to accomplish each of the requirements identified in the PWS." Given that the PWS requirements consist of 29 detailed CLINS, will the will the Government consider increasing the 45-page limit so that offerors can comprehensively present their approach and adequately address the requirement?

Answer*:** ***No.

149. The RFP, page 7 states that "The United States (U.S.) citizenship status of all known individuals proposed to perform and fill positions. Positions to be filled by future identified proposed staffing shall also include such identification to illustrate the contractor's intent. In addition, the chart shall include the identification of the overall percentage, in numerical format, of proposed U.S. citizens and non-U.S. citizens." Will the Government consider removing the requirement for the offeror to provide the citizenship status of proposed staff and future identified personnel, as it gives an unfair advantage to the incumbent?

Answer*:** ***No. Refer to the response to question #15 for additional information.

150. The RFP, Page 8, 3(b), 1st paragraph, last sentence, states that "The performance references shall be within the last three years." Is it acceptable to include contracts/task orders that are ongoing, but where multiple option periods have been completed?

Answer*:** ***Yes.

151. The RFP, Page 8, 3(b), 2nd paragraph, 1st sentence states "Furthermore, the ASB prime contractor is required to include within the three references identified above at least one project supporting a Federal Agency that the ASB prime contractor performed and completed as the prime with an annual value of no less than $2 million." Please confirm that the $2 million requirement is an average annual value over the duration of the contract.

Answer*:** ***Confirmation denied. The minimum value for each annual period of performance included within the reference shall be no less than $2 million.

152. The RFP, Page 8, 3(b), 2nd paragraph, 2nd sentence states that "if the ASB prime contractor is a Joint Venture (JV) company that has no relevant past/present performance, which shall be clearly stated within the proposal, then the Government may consider one reference from one partner of the JV to meet the requirement in the preceding sentence regarding minimum performance requirements as a prime contractor." If a JV partner has completed most of a contract (e.g., has completed four out of five years on a contract), will that contract be considered acceptable as far as meeting the criteria to be "performed and completed"?

Answer*:** ***The RFP has been revised to reflect the deletion of the terminology "and completed".

153. The RFP, page 8, 3 (c) states that "If applicable, the submittal in this section shall also list any contract or purchase order under which either a cure notice or show cause letter was received, or any contract or purchase order that was terminated for cause by the Government within the past three years." Please confirm that this is only required for the prime contractor?

Answer*:** ***Confirmation denied. Such information is required for all contractors (prime contractor, subcontractor, joint venture partners, etc.) included within the proposed staffing plan.

154. The RFP, page 12, "Due Date" says that "Electronic copies must be submitted no later than the date established in eBuy, with six hardcopies to be delivered within 24 hours of this date/time…". The due date established in eBuy is Friday, January 30. This would mean that the hardcopies would need to be delivered within 24 hours (i.e., on Saturday, January 31) but most Government offices are closed on Saturdays. Please confirm the due date/time for electronic submission? Please confirm that the requirement for hard copies is for delivery within 24 business hours, and that hard copies can be delivered on Monday, February 2, by 5:00 p.m.

Answer*:** ***Refer to the response to question #35.

155. The RFP, page 12, "Due Date" says that "Electronic copies must be submitted no later than the date established in eBuy, with six hardcopies to be delivered within 24 hours of this date/time…". Other than the number of copies, are there any other instructions regarding the hardcopy submission (e.g., packaging, binders, tabs, single-sided paper).

Answer*:** ***The hard copy submittal shall be consistent with the electronic submission as per the instructions in RFP paragraph (III)(A)(3).

156. The RFP, page 12, "Due Date" says that "Electronic copies must be submitted no later than the date established in eBuy, with six hardcopies to be delivered within 24 hours of this date/time…". Are there any special instructions for: a) Hardcopy delivery via courier? And b) Hardcopy delivery via mail?

Answer*:** ***No.

157. The RFP Attachment 1 – PWS Attachment C is an excel spreadsheet listing the 29 CLINS and estimated FTE count. Can the Government confirm that all potential bidders are required to propose the FTEs outlined in the RFP Attachment 1 – PWS Attachment C?

Answer*:** ***Refer to the response to question #14.

158. The RFP Attachment 1 – PWS Attachment A: CLIN 001 - Audit Support Services & CLIN 006 - Information Systems Security Support Services. Within Section 2 Scope/Duties, item b, there is a hyperlink to Appendix E - Security Controls Assessment List and a hyperlink foot note for the USDA Six Step Risk Management Framework Process (RMF) Guide. To better enable us to analyze the scope and duties associated with this CLIN, could the Government please provide these references?

Answer*:** ***Refer to the response to question #56.

159. The RFP Attachment 1 – PWS Attachment A: CLIN 003 - Business Continuity Planning Services. Section 2 Scope/Duties item c) states that 2 tabletop exercises are performed annually and 1 tabletop exercise is performed monthly. Can the Government provide additional information regarding the scope of each of these tabletop exercises, clarifying the differences between those performed monthly and those performed annually?

Answer*:** ***The annual tabletop exercises are comprehensive technical walkthroughs. The monthly tabletop exercises are customer requested walkthroughs of the customers DR plans that present general problems with the IT systems that individuals answer based on their role within the organization.

160. The PWS, page 6, 5.1, lists 29 CLINs.

a) Are these CLINs the same CLINs on the existing contract?

<u>Answer</u>: The current task order contains CLINs that provide similar services; however, the CLIN names and or tasks have been revised as required.

b) If not, how many, and which, additional CLINs have been added, or deleted?

<u>Answer</u>: The table below identifies the CLINs included in the current task order.

CLIN	Title/Description
001	Business Continuity Planning Services
003	Configuration Management Specialist - Technical Writer
008	Mainframe Network Systems Support - I
011	Network Management Specialist
012	Project Manager - MS Project
015	Senior Information Systems Security (ISS) Specialist - III
016	Software Engineer
018	Websphere Support
019	System Administration
020	SAN Administrator
022	Project Manager
023	Equipment Specialist
024	Agency Liaison/Software Specialist/Technical Architect
025	Network Security
026	RACF Support
027	Systems/Application Integrator and Performance Manager Requirements
031	Safeboot Encryption Specialist
032a	Security Administrator/Active Directory
033	Remedy Engineer
035	Enterprise Search Engineer
036	E-Gov Websphere Integration Engineer
037	Database Engineer-Oracle
039	Personnel Security Specialist
040	Information Services Consultant
041	Audit Specialist
042	IT Budget Systems Analyst
043	Database Administration Support
044	BladeLogic Administrator
045	ITIL SACM- Change Analyst
046	Capacity Management Specialist
047	Senior Level Application Business Analyst
048	Integration Subject Matter Expert
049	ADDM System Engineer
051	Telecom X.25 Network Specialist
052	Security Administrator- Junior/Active Directory/Identity Management Specialist

161. Pricing /Attachment 2.

a) Confirm that rows can be added to the spreadsheet, per notations in cells in Attachment 2? When attempting to do so, row and column calculations do not update accordingly.

<u>Answer</u>: Rows can be added. It is the contractor's responsibility to update formulas accordingly and as required to ensure the accuracy of pricing information. The identification

of pricing errors may result in the contractor's submission not being further evaluated for award purposes.

b) Can the bidder make other changes to Attachment 2?

***Answer:* No.**

c) On the "Totals" tab, column B "Transition Period" is blacked out and the cell formulas link to empty cells on the "FFP" tab. Please confirm--are these correct?

***Answer:* The template is correct.**

d) On the "Totals" tab, row 34, please describe the costs associated with "CAF" in the amount of $100,000.

***Answer:* The "CAF" is the ASB Contract Access Fee, which has an annual cap of $100,000.**

162. RFP, Section IV, Proposal Content, 4.e states "Travel. The Government's estimated travel cost for each performance period is listed in the Government provided template. The proposal shall identify any indirect cost related to the travel other direct costs. The proposal shall include a copy of the Defense Contract Audit Agency (DCAA) approval letter for any indirect rates (i.e. G&A, etc.)". Are Small Business Contractors "required" to have DCAA approved indirect rates, supported by DCAA Approval letter? Is a satisfactory incurred cost submission audit and documentation of such acceptable?.

***Answer:* The contractor is not required to have DCAA approved indirect rates. If the proposed indirect rates have been audited and approved by an authorized Government agency, evidence of such shall be submitted. The lack of such evidence will require such rates to be determined fair and reasonable by the Contracting Officer, prior to award of any resultant task order.**

163. The RFP, Page 10, Evaluation Criteria, Factor 3. Will the Government's award decision be based on total cumulative price for the full five (5) years or only the base year?

***Answer:* The total evaluated price/cost will be obtained from the pricing template (cell H45 on the "totals" sheet).**

164. The RFP, page 10, Evaluation Criteria, Factor 3. Will the "FFP – Transition Period" price be considered as part of the total evaluated price?

***Answer:* Refer to the response to question #163.**

165. RFP/p.4/II. We typically integrate our DCAA letter as an image into the MS Word/PDF document. This will NOT be searchable as text since it's a scan of a hard copy letter. Please confirm that this is acceptable in light of this minimum requirement and, if not, how we should address this issue in our electronic response.

***Answer:* Such approach is acceptable.**

166. RFP/p.4/III(A). Are vendors required to input pricing information into eBuy, or is the price proposal document and attachment sufficient?

***Answer:* Pricing information is required to be submitted in eBuy.**

167. RFP/p.4/III(A)(1) and RFP/pp.6–7/ IV(B)(2)(c)(ii). "The organizational chart shall be printed on paper of sufficient size to allow the entire chart to be displayed on a single page." An organizational chart produced using a product such as Visio, with the level of detail required by the RFP, will be very difficult to fit on a single sheet of paper. Can we propose providing a high-level organizational

chart, with a table or tables providing the detailed information required per the RFP instructions on pp. 6–7?

***Answer**: No.*

168. RFP/p.5/IV(A)(3). Please confirm the inclusion or exclusion of the following from the 45-page proposal content limit.

- Title page
- Table of contents
- Cover letter
- Organizational chart
- Resumes
- 2-page past performance references provided by the Contractor

***Answer**: Confirmation partially denied. As per the RFP, said information, with the exception of the standalone cover letter document/file, shall be included within the established page limitation.*

169. RFP/p.5/IV(B)(1)(a). To what does "Business Size" refer (e.g., small vs. large, annual revenue, number of employees)?

***Answer**: The business size shall identify the contractor as either a large business or a small business.*

170. RFP/p.7/IV(B)(2)(c)(ii). What is the page limit per resume, if any?

***Answer**: There is not a page limitation established for resumes.*

171. RFP/p.8/IV(B)(3)(b)(v). Must the contract value be broken down to show the amount paid for the base period and for each option year separately?

***Answer**: Use of RFP Attachment 2 (pricing template) is required.*

172. RFP/p.9/IV/General. Will USDA allow semi-monthly billing?

***Answer**: No.*

173. RFP/p.9/IV/General. If our actual calculated CAF is below the assigned 100K, are we to adjust it to actual?

***Answer**: Yes.*

174. RFP/p.9/IV(B)(4)(b). Since the Government estimate used 1,920 as the basis for an FTE, please confirm that all bidders must use 1,920 as well to level-set the pricing models across CLINs.

***Answer**: Confirmation denied. Refer to the response to question #14.*

175. RFP/p.9/IV(B)(4)(e). "The proposal shall include a copy of the Defense Contract Audit Agency (DCAA) approval letter for any indirect rates (i.e., G&A, etc.)."Our DCAA letter is several pages long itself. Can the Contractor's DCAA approval letter be excluded from the price proposal 5-page limit?

***Answer**: Yes. The indirect rate documentation shall be included within the price proposal submission; however, it is excluded from the established page limitation.*

176. RFP/p.9/IV(B)(4)(e). Is a DCAA approval letter required by the Prime at time of submission?

***Answer**: Refer to the response to questions #162 and #175.*

177. RFP/p.9/IV(B)(4)(e). Is a DCAA approval letter required by any subcontractors at the time of submission?

***Answer:* No.**

178. PWS/p.10/8.5. Does the requirement to provide "labor hours expended" include the FFP CLINs or only the LH CLINs?

***Answer:* Refer to the response to question #64.**

179. Can you provide the current level of staffing for the FFP CLINs (001 to 012)?

***Answer:* The current task order doesn't include FFP CLINs. Refer to the response to question #160 for information regarding current CLINs. The estimated core FTE numbers identified in PWS Attachment C are considered to be similar to the current level of support for the majority of the CLINs.**

180. Can the past performance requirements for all "Alliant Small Business contractors with the requirement for at least one project supporting a Federal Agency that the ASB prime contractor performed and completed as the prime with an annual value of no less than $2 million" be applied to all ASB contractors uniformly including ASB Joint ventures.

***Answer:* The evaluation criteria and corresponding requirements will be applied consistently to all submissions received in response to the RFP.**

181. Ref. RFQ Section IV, Paragraph 2, Subparagraph (c), Section (ii), page 7: The RFP requires inclusion of resumes for personnel fulfilling key positions. Are resumes included in the page count allocated to the Technical Volume?

***Answer:* Yes.**

182. Ref. Same section as above: Additionally, is there a page limitation for individual resumes.

***Answer:* No, there is not a page limitation established for resumes.**

183. In the RFP ID05140054, Section IV. PROPOSAL CONTENT, under Item B. Detailed, page 8, Paragraph 3. Past Experience and Performance (part of the technical proposal), item b) stated "Furthermore, the ASB prime contractor is required to include (within the three references identified above) at least one project supporting a Federal Agency that the ASB prime contractor performed and completed as the prime with an annual value of no less than $2 million.". Contradictorily, on page 9, item f) stated "Offerors with no relevant past or present performance history shall receive the rating of "neutral" meaning the rating is treated neither favorably nor unfavorably." **Please clarify if a prime contract holder of GSA Alliant SB GWAC without a project with annual value of no less than $2 million is eligible to submit the proposal response for this. Or Does this indicate that if our past performance within the last 3 years does not exceeding $2M we can still submit a qualifying RFP response?**

Answer: The RFP is clear that the ASB prime contractor is required to include (within the three references identified in paragraph b) at least one project supporting a Federal Agency that the ASB prime contractor performed as the prime with an annual value, for each annual period of performance included within the project, of no less than $2 million. If the ASB prime contractor is a Joint Venture (JV) company that has no relevant past/present performance, which shall be clearly stated within the proposal, then the Government may consider one reference from one partner of the JV to meet the requirement in the preceding sentence regarding minimum performance requirements as a prime contractor**.**

184. The RFP response due date and time is now set up as 01/30/2015 05:00:00 PM EST. Considering the answers to the questions have not been released as of now, compounded with there are some federal holidays between the RFP release date and proposal submission date, can the government extend the response window by 3 weeks to allow enough time for teaming and ensuring a quality proposal preparation?

***Answer*: Refer to the revised RFP closing date established in the eBuy system.**

185. Does the USDA have an opinion or preference regarding the number of key positions that should be proposed, based on current activity?

***Answer*: Refer to the response to question #30.**

186. Can the USDA provide additional detail regarding the level of experience required for each of the positions detailed in PWS Attachment C?

***Answer*: Applicable experience requirements are identified within the CLIN documents.**

187. We have past performance contracts exceeding the $2M requirement, but not within the last 3 years. Will the USDA/GSA extend the past performance duration to X years and/or lower the requirement to $1.5M?

***Answer*: No.**

188. RFP IV. B. 2. ii (p. 7) Please confirm that resumes for key positions are outside page limitations.

***Answer*: Confirmation denied. The resumes are included within the established page limitation.**

189. RFP IV. B. 2. iii (p. 7)Please confirm that the LCATs and ASB skill level descriptions are outside page limitations.

***Answer*: Refer to the response to question #9.**

USDA Six Step Risk Management Framework (RMF) Process Guide

Agriculture Security Operations Center (ASOC)

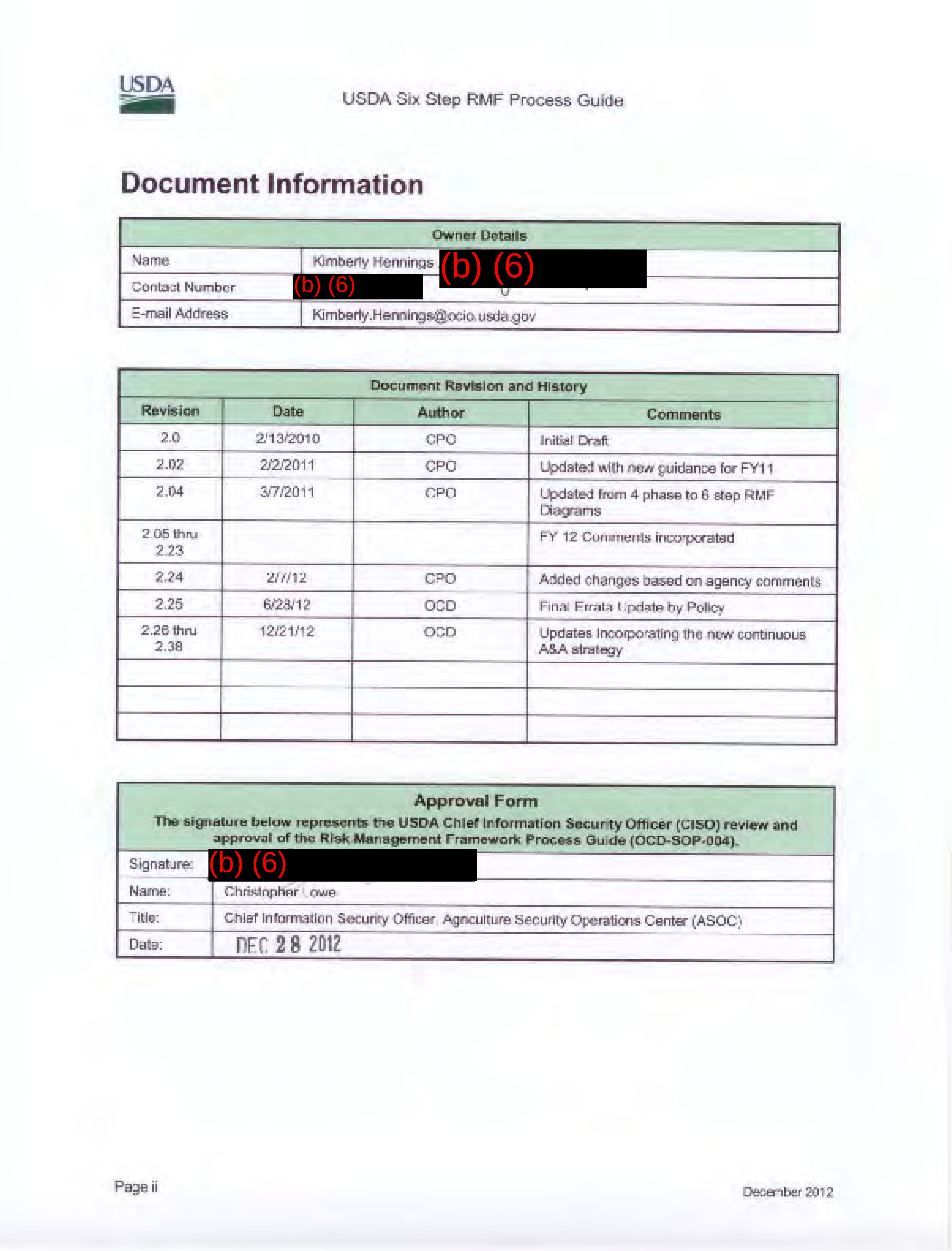
Oversight Compliance Division (OCD)

Revision: 2.38

December 2012

OCD-SOP-004

United States Department of Agriculture
1400 Independence Ave., SW
Washington, DC 20250



Document Information

Owner Details	
Name	Kimberly Hennings (b) (6)
Contact Number	(b) (6)
E-mail Address	Kimberly.Hennings@ocio.usda.gov

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
2.0	2/13/2010	CPO	Initial Draft
2.02	2/2/2011	CPO	Updated with new guidance for FY11
2.04	3/7/2011	CPO	Updated from 4 phase to 6 step RMF Diagrams
2.05 thru 2.23			FY 12 Comments incorporated
2.24	2/7/12	CPO	Added changes based on agency comments
2.25	6/23/12	OCD	Final Errata Update by Policy
2.26 thru 2.38	12/21/12	OCD	Updates Incorporating the new continuous A&A strategy

Approval Form

The signature below represents the USDA Chief Information Security Officer (CISO) review and approval of the Risk Management Framework Process Guide (OCD-SOP-004).

Signature:	(b) (6)
Name:	Christopher Lowe
Title:	Chief Information Security Officer, Agriculture Security Operations Center (ASOC)
Date:	DEC 28 2012

Distribution List			
Name	**Title**	**Agency/Office**	**Contact Information**

Table of Contents

TABLE OF CONTENTS IV

1 INTRODUCTION 6

1.1 Summary (Updates/Changes) 6

1.1.1 Continuous Assessment and Authorization Status 6

1.1.2 Updates to General Guidance on A&A 8

1.2 Purpose 9

2 RISK MANAGEMENT FRAMEWORK 11

2.1 Step 1: Categorize the Program/System 11

2.1.1 Collect System Information 12

2.1.2 Perform PTA, optionally the PIA 12

2.1.3 Security Categorization 13

2.1.4 Step1 Completion Summary 14

2.2 Step Two: Select Security Controls 15

2.2.1 Identify Common/Hybrid Controls 16

2.2.2 Tailoring Remaining Controls and Document in CSAM 17

2.2.3 Develop a Strategy for Monitoring the Controls 18

2.2.4 Step 2 Completion Summary 18

2.3 Step 3a: Implement Security Controls 18

2.3.1 Step 3.1: Implement Security Controls 19

2.3.2 Step 3.2: Update the SSP 19

2.3.3 Step 3.3: Finalize the CP, CMP and IRP 20

2.4 Step 3b: Concurrency Review 20

2.5 Step 4a: Assess Security Controls 21

2.5.1 Develop a Security Assessment Plan 23

2.5.2 Perform the Security Controls Assessment 24

2.5.3 Develop/Review Security Assessment Report, Risk Assessment and POA&Ms 27

2.5.4 Risk Based Decisions (RBD) 27

2.5.5 Step 4 Completion Summary 28

2.6 Step 4b: Submit the Package for Final Concurrency Review 29

2.6.1 Authority to Test 30

2.7 Step 5: Authorize Information System 30

2.8 Step 6: Monitor Security Controls 32

2.8.1 Continuous Monitoring Process Overview 32

2.8.2 Significant (Major) Change Definition 34

2.8.3 Transition to Continuous Assessment and Authorization 36

2.8.4 Continuous Assessment/Continuous Monitoring Process 37

2.8.5 Clearing POA&Ms and Updating the Risk Assessment 39

3 A&A DOCUMENTS, PROCESSES AND INFORMATION 40

3.1 CSAM Appendices and the CSAM Status Page 40

3.2 Configuration Management Plan 45
3.3 Contingency Plan 45
3.3.1 Contingency Plan Testing 45
3.4 Disaster Recovery Plan 46
3.5 Interconnection Security Agreement 47
3.6 E-Authentication Risk Assessment 47
3.7 Incident Response Plan 47
3.8 Concurrency Review 47
3.9 Plan of Action and Milestones 48
3.10 Documenting Contractor Provided Services (Systems) in CSAM 48

4 CONTACT INFORMATION 50

APPENDIX A - ACRONYMS 52

APPENDIX B - A&A TEMPLATES 53

APPENDIX C – CONCURRENCY REVIEW CHECKLISTS 54

APPENDIX D – GUIDES 55

APPENDIX E – IT SECURITY CONTROLS FOR ASSESSMENT 56

Tables

Table 1 - Step 1 Requirements Summary 11
Table 2 –1 Annual Monitoring Tasks 32

Figures

Figure 1-1: USDA Six Step RMF Process Flow 10
Figure 2-1: RMF Step 1 – Categorization 12
Figure 2-2: RMF Step 2 - Select Security Controls 15
Figure 2-3: RMF Step 3 - Implement Security Controls 19
Figure 2-4: RMF Step 4 - Assess Security Controls 23
Figure 2-5: RMF Step 5 - Authorize Security Controls 31
Figure 2-6: RMF Step 6 - Monitor Security Controls 33
Figure 2-7: Continuous Assessment and Authorization Tasks 34
Figure 2-8: Transition into Continuous Assessment/Authorization 37

1 Introduction

The Office of the Chief Information Officer (OCIO), Agriculture Security Operations Center (ASOC), Oversight Compliance Division (OCD) provides oversight for the United States Department of Agriculture's (USDA) Assessment and Authorization (A&A) program, formerly known as the Certification and Accreditation (C&A) program. The program is based on guidance provided in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision (Rev.) 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*; mandates identified in the Federal Information Processing Standards (FIPS) Publication (Pub)199, *Standards for Security Categorization of Federal Information and Information Systems*; FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems*; and USDA enhancements created to accommodate the Department's environment.

The intent of the A&A process is to evaluate Information Technology (IT) systems against documented specific information security requirements, verify information security control test results, summarize the residual risk, and involve the Department's senior management (the System Owner and the Authorizing Official (AO)) in the security lifecycle of the system.

This guide is designed to lead System Owners and certification and risk assessment teams through the USDA's A&A process. It provides a basic understanding of the process steps and examples of what information to input (system information and documents) into the Cyber Security Assessment Management System (CSAM).

This document relies on additional resources such as templates, checklists and guides that provide guidance on the details of the process. These appendices are organized into:

- Appendix A - Acronyms
- Links are provided for the following appendices:
    - Appendix B – A&A Templates
    - Appendix C – Concurrency Review Templates
    - Appendix D – User's Guide(s) (CSAM, POA&M, Retirement)

1.1 Summary (Updates/Changes)

This document applies to all USDA IT systems (and programs) including contractor systems operated or maintained on behalf of USDA. All System Owners are required to follow the steps identified in this manual to successfully complete A&A for their IT systems and major applications, input the information and results in CSAM, and authorize the system/application for operation. The following list summarizes the important changes/aspects of the process:

1.1.1 Continuous Assessment and Authorization Status

The Department has begun the migration to continuous assessment and authorization (A&A) in fiscal year (FY) 2013. The "Continuous Monitoring A&A Workgroup" (A Department wide team) was formed to finalize the process, control sets and periodicity of testing. The following information outlines the processes the Department will be utilizing to migrate to the NIST RMF continuous A&A requirements:

- Systems authorized in FY 2012 will immediately enter annual A&A and only be required to assess the set of controls specified by the Department every FY.
- All systems requiring authorization in FY 2013 must complete A&A (Steps 1-5) and test all their controls. Once these systems have successfully completed the full and traditional A&A process, they will enter into the continuous A&A methodology.
- All systems requiring authorization in FY 2014 must assess the identified set of security controls for FY 2013, and the remainder during their normal Authorization to Operate (ATO) testing in FY 2014 before entering continuous A&A.
- The Department will issue a set of controls to be assessed (roughly one-third of the controls each year) for the next three years. This year's controls were finalized by the "Continuous Monitoring A&A Workgroup" and issued in early December 2012. Future FY continuous A&A control sets will be issued no later than October 31st of each new fiscal year thereafter. The A-123 specific controls will be issued directly by the OCFO for FY 2013.
- Once systems have entered an annual assessment and authorization state:
    - System owners will review and update their system and program security plans in CSAM to specifically address the designated controls and then submit the system security plans (SSP) to the ASOC OCD (formerly Cyber Policy & Oversight) for concurrence review. Concurrence review staff will review the SSP, concentrating on the designated controls for that FY and then issue a formal concur memo so that testing may commence.□ Agencies/System Owners must submit their test results and documentation for RMF Step 4 concurrence review and address any deficiencies before receiving an annual concur memo documenting the completion of the process for that year.
    - All FY 2012 and FY 2014 systems, including contractor systems, must have all annual assessment activities completed and submitted to concurrency review no later than August 31, 2013
    - Documentation for contractor provided services (systems) must be entered into CSAM no later than 3/31/12 (See section 3.10 of this guide)
    - The above steps shall be completed as defined in the USDA Six Step RMF Process Guide.
    - For moderate or high systems, all controls must be assessed by an independent assessor. Based on the definition of an independent assessor provided in "NIST SP 800-37 Revision 1 , Page 30, section 3.4", the USDA provides the following guidance on defining an independent assessor:
        - An independent assessor is one who is impartial and not influenced by the system owner or their direct staff during the conduct of the assessment of security controls or the reporting of the results.
        - Independent assessors and/or assessment teams may be in-house permanent teams or outsourced as needed. However the services are

performed, strict measures must be put in place to obtain an impartial assessment result.

    - To obtain impartiality, the system owner should not be directly involved in the management of, or contracting for, the assessment services. If this cannot be done, the system owner must put in place strict measures and/or contracting language to ensure that they cannot influence said assessment services.
    - The assessor (contractor's company) cannot be directly or indirectly involved in the development, management, or operation of the security controls to be assessed.
    - If a system is working through RMF steps 4 through 6, assessment of this system must be performed by a different contractor than the one that performed RMF steps 1 through 3.
  - The authorizing official can further add to this defined level of assessor independence, but cannot prescribe less stringent requirements. Additional requirements should be based on the value (security categorization) of the data contained within the system, the value of the operational output, or the criticality of the system to the USDA and/or information technology infrastructure of the United States.

1.1.2 Updates to General Guidance on A&A

- All systems designated as Federal Information Security Management Act (FISMA) reportable must be recorded in CSAM and must have an OMB 300 unique project identifier (UPI) or unique investment identifier code (working capital fund number).
- All systems placed in "Modification" Status will have their corresponding ATO status set to "None".
- All systems that are funded by the USDA and/or transmit, process or store USDA data are required to go through the USDA RMF assessment and accreditation process as defined in USDA Six Step RMF Process Guide.
- ASOC OCD will review any system (including FedRAMP) external to the agency that hosts USDA systems and/or data determining the degree of acceptability of compliance with the USDA RMF process
- All systems submitted for concurrence review must fully utilize the CSAM tool and comply with all requirements in the USDA RMF guide. Scanned copies of all applicable document signature pages must be uploaded into CSAM or inserted into their respective document.
- All programs are subject to the USDA RMF process and must complete the same steps as a system, including concurrence reviews and subsequent issuance of an ATO. As not all the documentation utilized for a system is pertinent to a program, additional specifics will be issued in FY 2013.
- All programs are required to complete steps 1 through 5 of the RMF process as defined in the USDA Six Step RMF Process Guide this fiscal year. In CSAM, all

programs will now show an expired ATO status until they have completed the A&A process.

- The following NIST SP 800-53 controls are system-specific controls and cannot be common, hybrid, or not applicable: CA-2, CA-2(1), CA-2(2), CA-3, CA-5, CA-6, PL-2, PL-5, RA-2, RA-3, SA-5, SA-5(1), SA-5(2), and SA-5(3).
- Systems categorized as moderate or high must have or be covered by their own or another system's configuration management plan (CMP). If a system is covered by another CMP, the plan providing the coverage must explicitly identify the covered system(s) by name and detail the extent of coverage.
- Security assessments must be fully documented. Detailed evidence of test accomplishments must be entered into CSAM for each and every applicable assessment. This must include date, time, who, and what was determined for interviews or tests performed.
- An Interconnection Security Agreement (ISA) and/or Memorandum of Understanding (MOU) is required for every system interconnection where the systems have different authorizing officials. This requirement also applies to hosted and contractor systems. The ISA requirements may be included in the contract with the hosting facility (MOU/SLA). ISAs will be reviewed annually and be re-performed every three years or to coincide with the system’s ATO date, whichever is sooner.
- Agencies must submit completed A&A packages no later than 45 days after completion of assessment and final package preparation. Therefore, agencies must be vigilant when submitting systems for Step 4 concurrence review and promptly address any identified issues.
- Contingency Plan/Disaster Recovery Plan (CP/DRP) testing is required for every system and must be documented in CSAM. Test plans, results documents, signature pages, and memos must be uploaded into CSAM through the status and archive page, then into CSAM appendices. DRPs are required for all facilities and are also required to be uploaded to CSAM. All moderate and high systems may complete a tabletop test the first year, but must complete a functional contingency plan test by their second year of operation.
- All assessors must complete the OCIO ASOC OCD Concurrence Review Training before they can perform any RMF tasks on any USDA systems. Training must be accomplished annually and proof of attendance issued by the Oversight and Compliance Division.
- The updated RMF guide, templates, checklists and other associated guidance documents are located on the OCIO information technology (IT) security intranet site. These documents should be utilized when performing RMF system and program continuous monitoring activities.

1.2 Purpose

This guide provides the accepted methodology for conducting a NIST and USDA compliant A&A of IT systems and performing the corresponding CSAM data entry of all results and required documentation. NIST 800-37 Rev. 1 takes a slightly different approach to the A&A process by addressing the process in six steps instead of the four phases that were delineated in the original version of NIST 800-37. An evaluation of the process reveals that whether you do it in steps or phases, the methodology is the same. All USDA agencies must follow the six step approach to achieve an Authority to Operate (ATO) and to effectively manage risk for their systems. The Department uses CSAM as its automated FISMA management tool and the system of record to capture system information throughout the A&A process. At USDA, all system information, documentation, and assessment results require recording in CSAM.

Below is a diagram of the six step RMF process.

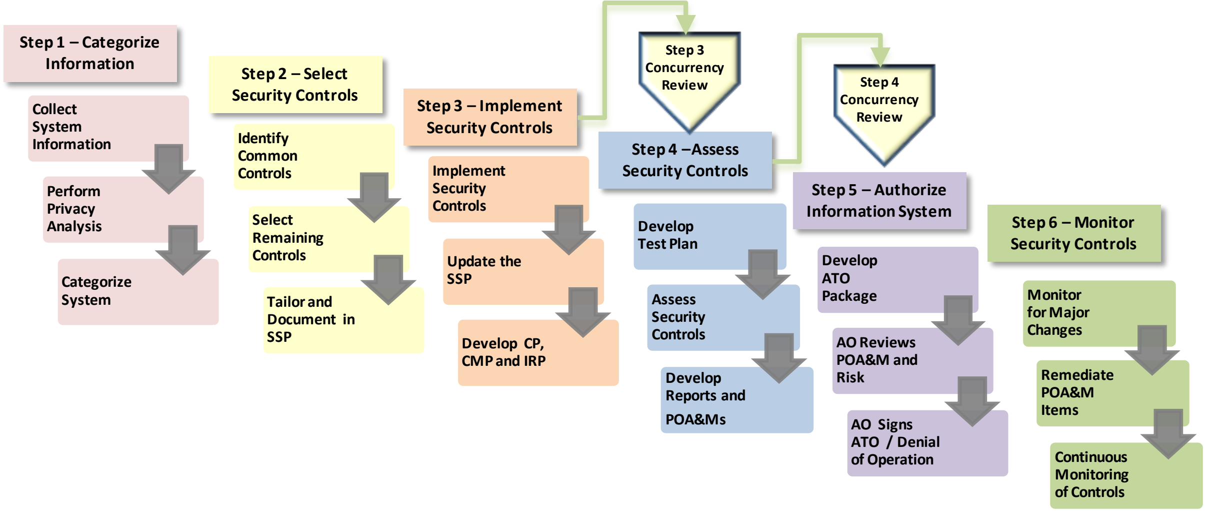

Step 1 – Categorize Information
Collect System Information
Perform Privacy Analysis
Categorize System
Step 2 – Select Security Controls
Identify Common Controls
Select Remaining Controls
Tailor and Document in SSP
Step 3 – Implement Security Controls
Implement Security Controls
Update the SSP
Develop CP, CMP and IRP
Step 3 Concurrency Review
Step 4 –Assess Security Controls
Develop Test Plan
Assess Security Controls
Develop Reports and POA&Ms
Step 4 Concurrency Review
Step 5 – Authorize Information System
Develop ATO Package
AO Reviews POA&M and Risk
AO Signs ATO / Denial of Operation
Step 6 – Monitor Security Controls
Monitor for Major Changes
Remediate POA&M Items
Continuous Monitoring of Controls

Figure 1-1: USDA Six Step RMF Process Flow

2 Risk Management Framework

Commencing with FY 2013, USDA is implementing a continuous assessment/continuous monitoring methodology of achieving a system/program ATO. Systems with ATO dates due during FY 2013 or earlier must complete the RMF steps as delineated below starting with Section 2.1. Systems with ATO dates that fall after FY 2013 shall follow the continuous authorization methodology as presented in Section 2.8.

2.1 Step 1: Categorize the Program/System

Step 1 of the RMF focuses on the collection of general system information, completing the Privacy Threshold Assessment (PTA), Privacy Impact Assessment (PIA) and completion of the FIPS 199 system categorization. This collected information includes the mission, environment, boundary definition, architecture, and information the system transmits or processes. The system owner is responsible for completing the categorization and may require the participation of the information system security officer or others as needed.

Requirements for All Systems/Programs	Potential Additional Requirements
• Collect general system information • Create CSAM entry and enter information • Create PTA and upload to CSAM • Perform security categorization • Enter remaining information in CSAM System Identification (Purpose, attributes, funding, etc.) and Narratives (System description and Technical description)	• Perform PIA and upload to CSAM • Perform E-Authentication Risk Assessment and upload to CSAM (under Appendix G5: E-Auth Risk Assessment OMB M04-04)

Table 1 - Step 1 Requirements Summary

Below is the overall process for RMF Step 1.

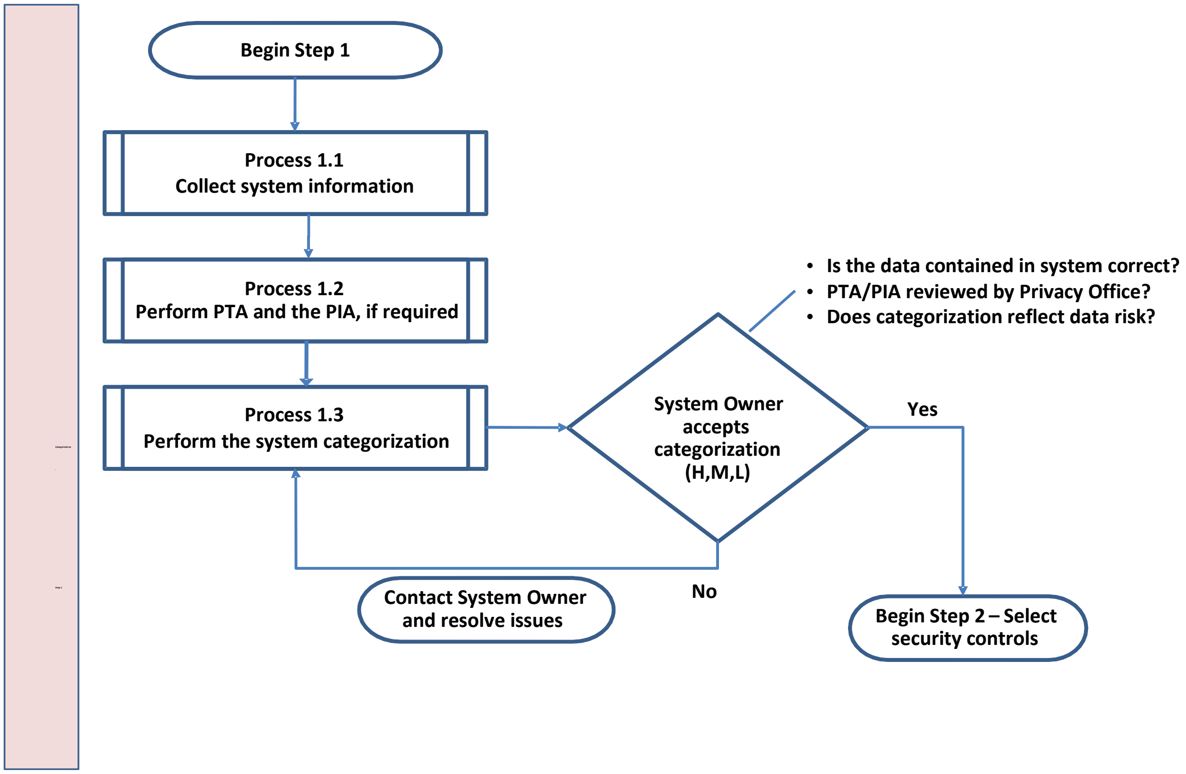

Begin Step 1
Process 1.1
Collect system information
Process 1.2
Perform PTA and the PIA, if required
Process 1.3
Perform the system categorization
System Owner accepts categorization (H,M,L)
• Is the data contained in system correct?
• PTA/PIA reviewed by Privacy Office?
• Does categorization reflect data risk?
Yes
No
Contact System Owner and resolve issues
Begin Step 2 – Select security controls

Figure 2-1: RMF Step 1 – Categorization

2.1.1 Collect System Information

Before beginning the categorization process, it is helpful to have the following information readily available: system and/or network diagrams; a description of the system's mission/purpose; business impact assessments; privacy impact threshold/privacy impact assessments; and contingency, disaster recovery, incident response, or configuration management plans. Systems in development will not have all of this documentation, but at a minimum will need to obtain information from the system's detailed design documentation.

While gathering information, it is best to start by populating the basic system information in CSAM. Any of this information can be updated as the system moves through the process. The CSAM headings of "System Information (Identification, Locations, Relationships, Narratives and Points of Contact", are areas that need to be filled out and completed before moving on to security categorization activities.

2.1.2 Perform PTA, optionally the PIA

With the information from section 2.1.1 gathered, perform a PTA based on the template in Appendix B. If indicated by the PTA, perform a PIA based on the template included in Appendix B. If privacy information and/or special handling is indicated by the PIA, then consideration of this is required during the next step - security categorization.

2.1.3 Security Categorization

The primary goal of this step is to utilize NIST SP-800-60 Rev.1, *Guide for Mapping Types of Information and Information Systems to Security Categories (Volume 1 and Volume 2)* in accordance with FIPS 199 to categorize the information system. The System Owner categorizes the information within the information system to determine the impact that a compromise of confidentiality, loss of integrity, and/or the lack of availability would have on the mission of the agency. This impact determination (low, moderate, or high) establishes the security control baseline applicable to the system. The system categorization is entered into CSAM from the " System Information" – "Information Types" section.

To perform a security categorization of any system requires knowledge of what information is contained within the system. It is important to determine the value of this information from the standpoint of confidentiality, integrity, and availability (CIA). This information is then utilized to determine the generic data categories from NIST SP 800-60 Revision 1 with their default values of high, moderate, or low for the CIA areas. The data categories equate to information types in CSAM. The default CIA values for each information type are also pre-populated in CSAM. Based on the value of the information in the system, these default values can be modified to be either more or less critical, as illustrated in the example below.

Once all the information types have been defined and values have been assigned, the overall categorization of the system is the highest value identified for any of the categories. This is referred to as the "high water mark". For any assigned values (low, moderate, high) that differ from the NIST recommended values, an explanation or justification must be entered that clearly explains the reason for the change from the NIST recommendation.

Systems that are made up of other systems/applications must include the information types for all the systems/applications involved. General support systems (GSS)/Major applications (MA) are categorized to the highest level of any of the applications/systems that reside on the GSS/MA.

Information Category	Confidentiality Rating (C) *(H,M,L)*	Integrity Rating (I) *(H,M,L)*	Availability Rating (A) *(H,M,L)*	Privacy	Financial	Medical	High Water Mark
Budget and Finance	M	M	L		X		
Immunization Management	M[1]	M	L	X		X	
**Highest Impact*	**M**	**M**	**L**	**X**	**X**	**X**	**M**

Footnotes:

[1] Some information associated with immunization management involves confidential patient information subject to the Privacy Act and to HIPAA.

Table 4: Example of FIPS 199 Categorization

2.1.4 Step1 Completion Summary

- Collect general information about the system, including specifics about what information the system will process, transmit, or store.
- Create a SSP entry in CSAM for the system and enter the general information.
- Perform a PTA based on the actual information contained in the system. If the PTA requires a PIA to be completed, then perform a PIA. Upload the PTA/PIA to CSAM.
- Perform the E-Authentication Risk Assessment and post it to Appendix G-5, if appropriate.
- Complete the categorization of the system in the CSAM Information Types tab by selecting the NIST 800-60 Revision 1 data categories that correspond to the actual information the system processes. If any risk levels (high, moderate or low) are changed for an information type, then document the reason.
- Completely describe the system by entering remaining information into CSAM to include the system's locations, interfaces, narratives, and points of contact.
- Register the system with other corresponding Departmental systems such as the Electronic Capital Investment Management Repository System (eCPIC) and/or Enterprise Architecture Repository (EAR). Ensure the OMB 300/53 identifier and name in CSAM matches those in the other systems.

2.2 Step Two: Select Security Controls

Just as FIPS 199 and NIST 800-60, Rev. 1 are mandatory for the categorization of information systems, FIPS 200 and NIST 800-53, Rev. 3 are mandatory for the selection of the corresponding security control baselines. Once the FIPS 199 security categorization of the information system is documented in CSAM, the corresponding set of controls (high, moderate or low) will automatically be selected for the information system within CSAM. This security control baseline must then be tailored within CSAM to include the selection of inherited controls and the documentation of the implementation of each control

Requirements for All Systems/Programs	Potential Additional Requirements
• Identification of all common/inherited controls • Compliance descriptions identified for every control including tailoring • Create any needed compensating controls • Develop Contingency Plan (CP), CP test training and testing documents	• 508 Compliance • System of Record Notice (SORN) • Configuration Management Plan(CMP) • Incident Response Plan (IRP) • Disaster Recovery Plan (DRP) • Interconnection Security Agreement (ISA) (Optionally this could be in the form of a Memorandum of Understanding (MOU) or Service Level Agreement (SLA))

Below is the overall process for RMF Step 2.

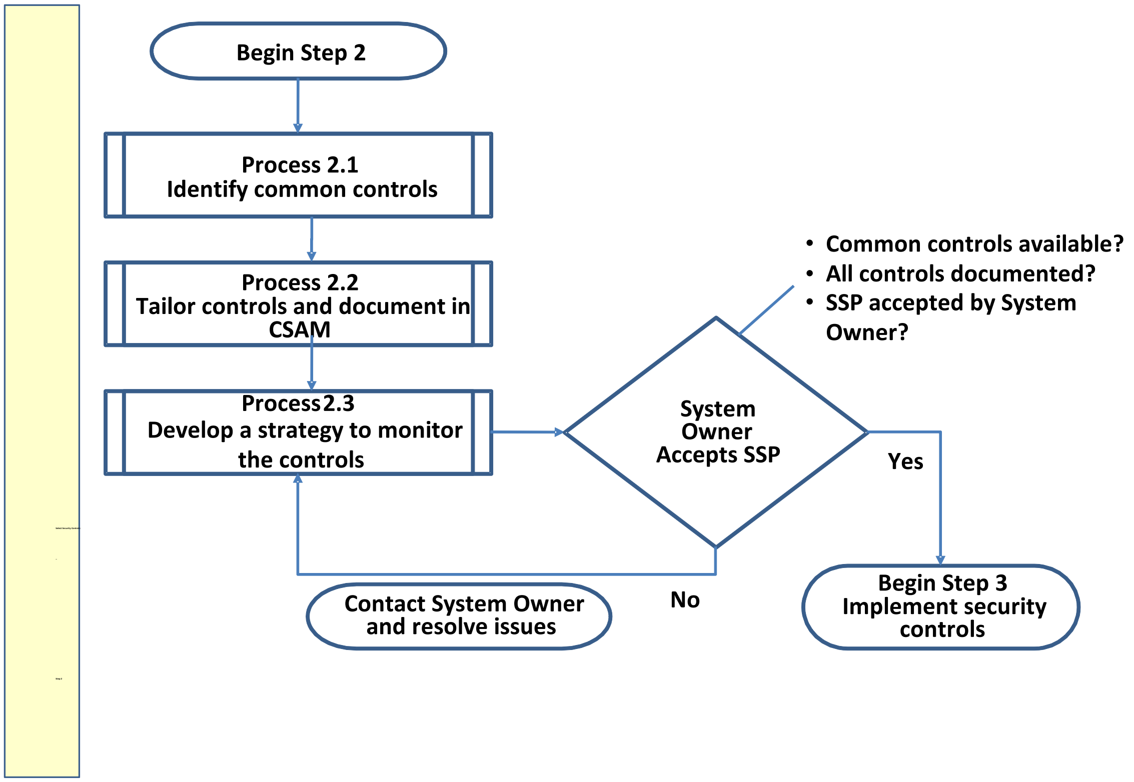

Begin Step 2
Process 2.1
Identify common controls
Process 2.2
Tailor controls and document in CSAM
Process2.3
Develop a strategy to monitor the controls
System Owner Accepts SSP
• Common controls available?
• All controls documented?
• SSP accepted by System Owner?
Yes
No
Contact System Owner and resolve issues
Begin Step 3
Implement security controls

Figure 2-2: RMF Step 2 - Select Security Controls

Step 2 focuses on completion of the compliance descriptions in CSAM for all security controls. The documentation includes the identification of all common controls, selection and documentation of the remaining controls, and any tailoring or compensating controls.

At USDA, identification of the controls the system can inherit is the responsibility of both the common controls provider and the system owner and/or ISSO/ISSPM. In the case of Department Program Management controls, this may involve the Department's CIO and/or CISO. The common controls provider must publish what controls are inheritable in CSAM and may also have them listed in other documents that are required by the data centers and/or other service providers. The controls are then formally documented as an appendix to the ISA which is then confirmed by signature by the common controls and/or data center provider.

2.2.1 Identify Common/Hybrid Controls

The selection of common controls is one of the first tasks that must be accomplished. A common control is a control that can be applied *in its entirety* to one or more organizational information systems. The control must be designated, assessed, and approved in writing as a common security control. There are a few points to remember when selecting common controls:

- Controls need to be inherited from the system that provides that service or capability. In other words, a Program does not actually perform virus scanning, so the virus scanning controls cannot be inherited from a Program. However, the virus scanning control could be inherited from the network or system the application resides on.
- Every common control (including the common portion of a hybrid control) must identify the exact Program/system that the control is common to. The Program/system should have: (1) a control implementation that satisfactorily documents the control in terms broad enough to include the systems that should inherit the control; and (2) tested the control as part of an A&A.
- Hybrid controls require a further explanation as to what is being inherited along with the name of the Program/system it is being inherited from.
- For NIST SP 800-53 Rev 3 the following restrictions exist:
    - Without exception, the following controls cannot be common, hybrid, or non-applicable (N/A): CA-2, CA-2(1), CA-2(2), CA-3, CA-5, CA-6, PL-2, PL-5, RA-2, RA-3, SA-5, SA-5(1), SA-5(2), and SA-5 (3).
    - The CP-2 control can be a common control if the CP for the system in question is: (1) a CP that covers multiple systems or a GSS; and (2) the control was previously tested during the assessment of another system covered by the CP. If the system has its own CP, it is a system specific control.
    - For most systems, the following audit controls would be system specific: AU-2, AU-2(3), and AU-2(4). There are some cases where the listing of what is audited can be partially inherited from the GSS, thus making the control hybrid.

- The Program Management (PM) family of controls can be inherited from the USDA Department Common Controls. The agencies should make any of these controls hybrid if they have additional policy or procedures that are pertinent to these controls.
- The Incident Response (IR) family of controls can be inherited from the USDA Department Common Controls. Agencies must be compliant with the policy and procedures as promulgated by the Department for this family.
- “Dash-1” controls -- the first control of each control family -- address Departmental policies and Agency procedures. The Dash-1 controls should be hybrid with the Department-level implementations offered by USDA Department Common Controls. The Department is responsible for the creation of the policies pertaining to the controls. The agencies are responsible for all control procedures, unless otherwise specified by the Department. Agencies may create policies that exceed the baseline guidance published by the Department but must follow Departmental policy (CA-1, IR-1, PM-1).

Common controls are selected and assigned in CSAM. As agencies update the systems with the proper inheritance issues may arise where a control implementation that is required to be inherited from a Program/system that is not set up in CSAM to allow the specific inheritance should be made "Not Applicable". When making the control not applicable, enter the complete explanation of the inheritance (what is inherited and from what system is it inherited from).

2.2.2 Tailoring Remaining Controls and Document in CSAM

Once the selection of common controls is accomplished, evaluate the remaining controls to determine which will be hybrid and which will be system specific. This is also a good opportunity to look at controls that are not applicable. Non-applicable controls must have a valid reason/justification explaining why they are not applicable. An example is the voice over Internet protocol (VOIP) control. This could be designated as not applicable because the system does not contain or use VOIP.

Once the decisions have been made as to what controls the system must implement, a strategy for continuous monitoring of the controls must be developed and any required changes to the control tailoring made. For a new system that has never been through the process, the Authorizing Official (AO) will approve the security plan at this point. This approval designates those controls that must be implemented by the system.

Most systems at USDA are operational with controls in place, therefore steps 1 through 3 for these systems has already been accomplished. For these systems, the SSP and associated documentation would just need to be reviewed/updated annually by the system owner.

2.2.3 Develop a Strategy for Monitoring the Controls

The Department establishes the criteria for selecting security controls to be monitored (post deployment) and determines the frequency of the monitoring for Key and annual sets of controls. The Department has established the monitoring criteria and frequency for all controls in the Department. (See Appendix E for the list of controls and the year of their assessment.) . The agency can monitor controls more frequently, but not less, that the Department baseline.

For FY 2013 and beyond, all control assessments for moderate/high categorized systems must be accomplished by an independent assessor, per NIST 800-53 Rev.3. The owner(s) of any controls inherited by the system is responsible for the annual assessment of those controls and the system will inherit the result.

2.2.4 Step 2 Completion Summary

- In the “Assessments – Control Management”, ensure the NIST Version is set to NIST SP 800-53 Rev3 and all the controls are on the system control set.
- Inherit common controls from those offered in the inheritance selection area for which you have permission.
- Enter compliance descriptions for all controls not inherited

2.3 Step 3a: Implement Security Controls

Step 3 focuses on the implementation of security controls during system development and/or after the system has been completed. Implementation of the security controls is the responsibility of the System Owner and/or the common controls provider where controls are inherited. Once the controls are implemented, the SSP compliance descriptions, CP, CMP and IRP should be finalized to capture the true “as-built” implementation. A CMP, IRP, and CP may need to be developed for the system unless these are covered under another plan elsewhere in the hosted environment.

Requirements for All Systems	Potential Additional Requirements
• Finalize SSP compliance descriptions • Finalize CP	• 508 Compliance • Finalize CMP, IRP and DRP (If required)

Below is the overall process for RMF Step 3a.

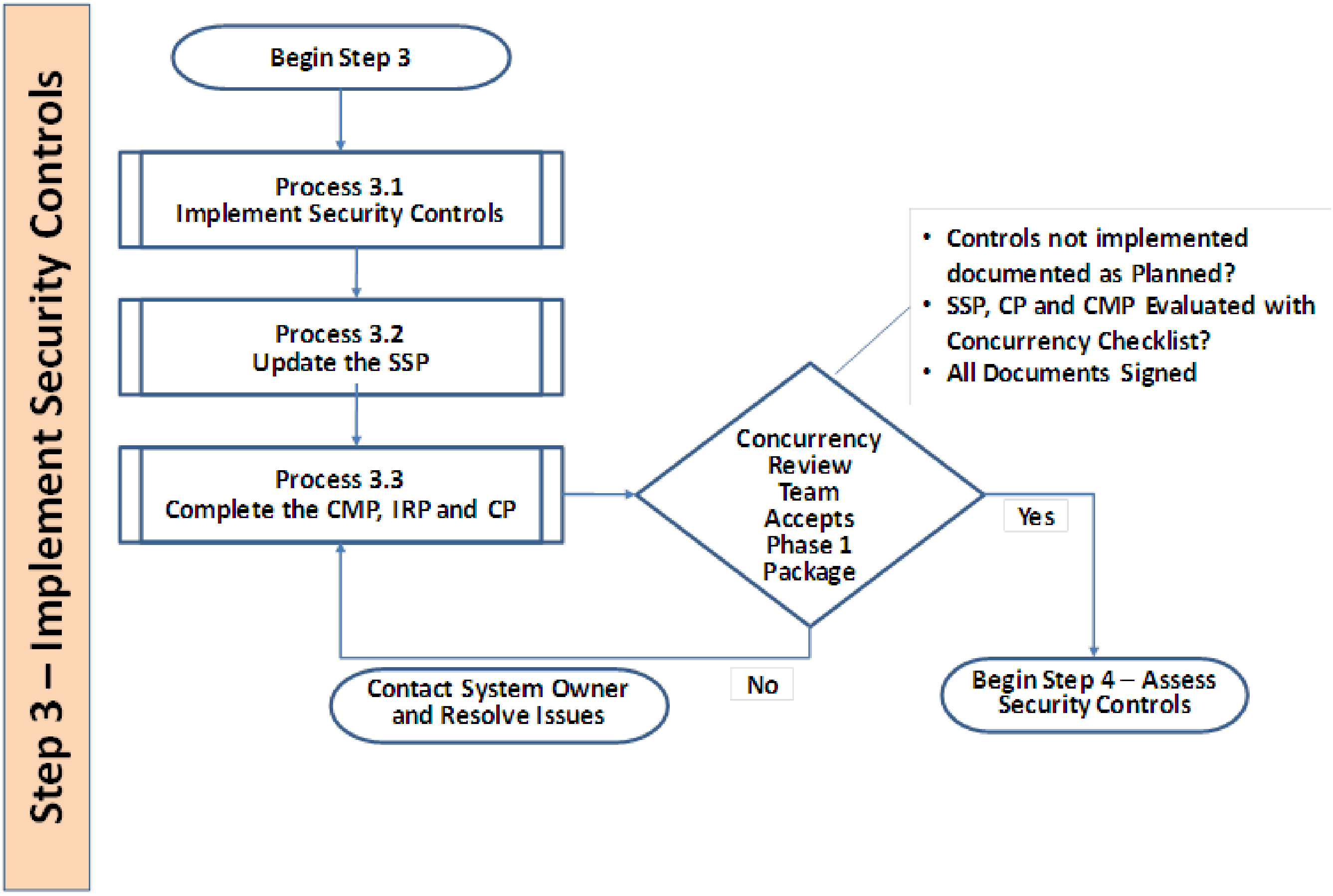

Step 3 – Implement Security Controls
Begin Step 3
Process 3.1
Implement Security Controls
Process 3.2
Update the SSP
Process 3.3
Complete the CMP, IRP and CP
Concurrency Review Team Accepts Phase 1 Package
• Controls not implemented documented as Planned?
• SSP, CP and CMP Evaluated with Concurrency Checklist?
• All Documents Signed
Yes
No
Contact System Owner and Resolve Issues
Begin Step 4 – Assess Security Controls

Figure 2-3: RMF Step 3 - Implement Security Controls

2.3.1 Step 3.1: Implement Security Controls

The primary task of this step is to document every applicable security control in the security plan. Be clear and address all aspects of the control. If the control has an A, B, and C, then the implementation should have an A, B, and C, followed by the implementation of each aspect of the control. This makes it easier for the security controls assessor and the concurrency review team to ensure that each aspect of a control is properly addressed and implemented. It is best to consider the NIST SP 800-53 control to be a statement of policy and the implementation a write-up of exactly how the Program/system implements this statement of policy. Therefore, it is unnecessary to quote policy in the implementation.

2.3.2 Step 3.2: Update the SSP

Once all the security controls are complete with implementations entered, generate the security plan in CSAM. Once generated, perform a review of the plan, checking to be sure that control implementations have indeed been entered into CSAM. Do a search of the plan for any blank fields. There should not be any. Every field should have something entered. If not, go back to the control implementation and determine why the field is blank.

2.3.3 Step 3.3: Finalize the CP, CMP and IRP

It is at this step that all the documents need to be updated to reflect the current state/implementation of the system. If the system is covered by an organizational CMP and IRP, then ensure these inherited documents contain specific references to the system. The CP should be finalized along with the CP test plan, training and CP test results. Specified inherited documentation should be specifically referenced as to their location, while system specific documentation can be loaded in CSAM to their Appendix locations following the guidance of Section 3.1.

Below is a checklist for Step 3 of major items that must be completed before submission for concurrency review:

- Finalize and post the CP, CP training, and CP test documentation to CSAM Status Page (Post to the CSAM System & Status Archive Page then to Appendix L).
- Finalize and post the IRP to the CSAM Appendix O. Either inherit it from the Department/agency or develop a system specific one.
- Finalize and post the CMP to the CSAM Appendix Q.
- Finalize and post an ISA/MOU/MOA to the "System Information" – "Relationships" tab for each system connection.
- Send an email to the Cyber Communication mailbox (Cyber.Communication@usda.gov) requesting a Step 3 Concurrency Review.

2.4 Step 3b: Concurrency Review

When the SSP is complete, it needs to be submitted for Step 3 concurrency review. The user submits an email to the concurrency review team at Cyber.Communication@usda.gov stating the package is ready for review in CSAM.

This concurrency review is primarily for the security plan and the categorization; however, the supporting documents (CP, CMP, ISA, PTA, and/or PIA) that are present at the time of the review will also be reviewed. If the concurrency review team finds any issues with the documentation, they will notate the issues in the concurrency review checklists and return the checklists to the agency. The key items for the Step 3 review are the system categorization and the security plan. Since Issues with the remaining documents do not have a significant effect on testing they can be addressed concurrently with performing Step 4 testing. The checklists utilized for concurrency review are located in Appendix C.

The result of the concurrency review is either passage of the system to Step 4 (Assess Security Controls), or the documentation is returned for further refinement with a checklist of items to remediate. Agencies cannot proceed to Step 4 until notified via concur memo that the system has successfully completed the Step 3b concurrency review. If the documentation is returned with a remediation checklist noting issues identified with the security plan, system categorization or other documents to be addressed, the system must be re-submitted to the concurrency review manager for verification that the issues have been adequately addressed. Upon satisfactory completion of concurrency review, the concurrency review manager will ensure that the RMF Step 3 concur memo is issued. Once the RMF Step 3 concur memo is issued, the SSP shall not be modified without first discussing the changes with the COE liaison and the concurrency review team. The SSP should not be unilaterally modified by the System Owner until after the Program/system is authorized to operate.

Below is a checklist for Step 3 concurrency review:

- Security plan/system notification submitted via email to the Cyber Communication mailbox for Step 3 concurrency review.
- Concurrency review comments for Step 3 received (completed checklists).
- Security plan/system updated based on concurrency review comments.
- Security plan/system re-submitted via email to the Cyber Communication mailbox for Step 3 concurrency re-review.
- Program/system Step 3 review completed (agency receives concur memo stating Step 3 concurrency review has passed).
- Program/system Concur Memorandum from ASOC OCD posted to the CSAM Status & Archive Page to Security Authorization section and then post to Appendix H.

Concurrency review will generate the Security Plan and post it to Appendix F*x* with titles "FY13 A&A Security Plan". "x" means the next consecutive numbered "F" appendix. (This is the A&A archive copy).

2.5 Step 4a: Assess Security Controls

The purpose of this step is to determine the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. This step also addresses specific actions to be taken or planned to correct deficiencies in the security controls, and to reduce or eliminate known vulnerabilities in the information system.

Please note that the RMF Step 4 (Assessment) for moderate/high systems must be performed by a different (independent) entity than the one utilized for RMF Steps 1-3 (Documentation and Implementation).

The term independent assessor is defined as follows:

- An independent assessor is one who is impartial and not influenced by the system owner or their direct staff during the conduct of the assessment of security controls or the reporting of the results.
- Independent assessors and/or assessment teams may be in-house permanent teams or outsourced as needed. However the services are performed, strict measures must be put in place to obtain an impartial assessment result.

- To obtain impartiality, the system owner should not be directly involved in the management of, or contracting for, the assessment services. If this cannot be done, the system owner must put in place strict measures and/or contracting language to ensure that they cannot influence said assessment services.
- The assessor (contractor's company) cannot be directly or indirectly involved in the development, management, or operation of the security controls to be assessed.
- If a system is working through RMF steps 4 through 6 for the first time, assessment of this system must be performed by a different contractor than the one that performed RMF steps 1 through 3.

The AO can further add to this defined level of assessor independence, but cannot prescribe less stringent requirements. Additional requirements should be based on the value (security categorization) of the data contained within the system, the value of the operational output, or the criticality of the system to the USDA and/or information technology infrastructure of the United States.

During Step 4, a certifier validates a system's compliance with the security controls as defined within the SSP. During the assessment of the system, utilizing the SSP as a guide to how the controls were implemented, the assessor may identify inconsistencies or errors within the SSP. The assessor is not authorized to make any changes to the SSP. The assessor should identify and clearly report these errors/inconsistencies to the System Owner, who will work with the concurrency review team to update the SSP. As stated earlier, once the Step 3b concur memo is received by the System Owner; no changes should be made to the system security plan without concurrence from the concurrency review team.

The security control assessment should be performed, the findings analyzed, and the security assessment report and residual risk reports generated in CSAM and forwarded to the agency Information System Security Program Manager (ISSPM) for use in Step 5 – Authorize Security Controls. The OCD concurrency review team and COE liaison must be invited to the Step 4 kick-off meeting.

Tasks Performed by Certifier	System Owner Requirements
• Develop Security Assessment Plan • Assess security controls • Analyze findings / quantify results • Develop/update Plans of Action and Milestones (POA&Ms)	• Provide certification coordination with Certifier • Ensure support system administration personnel are available during testing • Ensure system is ready for testing

Below is the overall process for RMF Step 4.

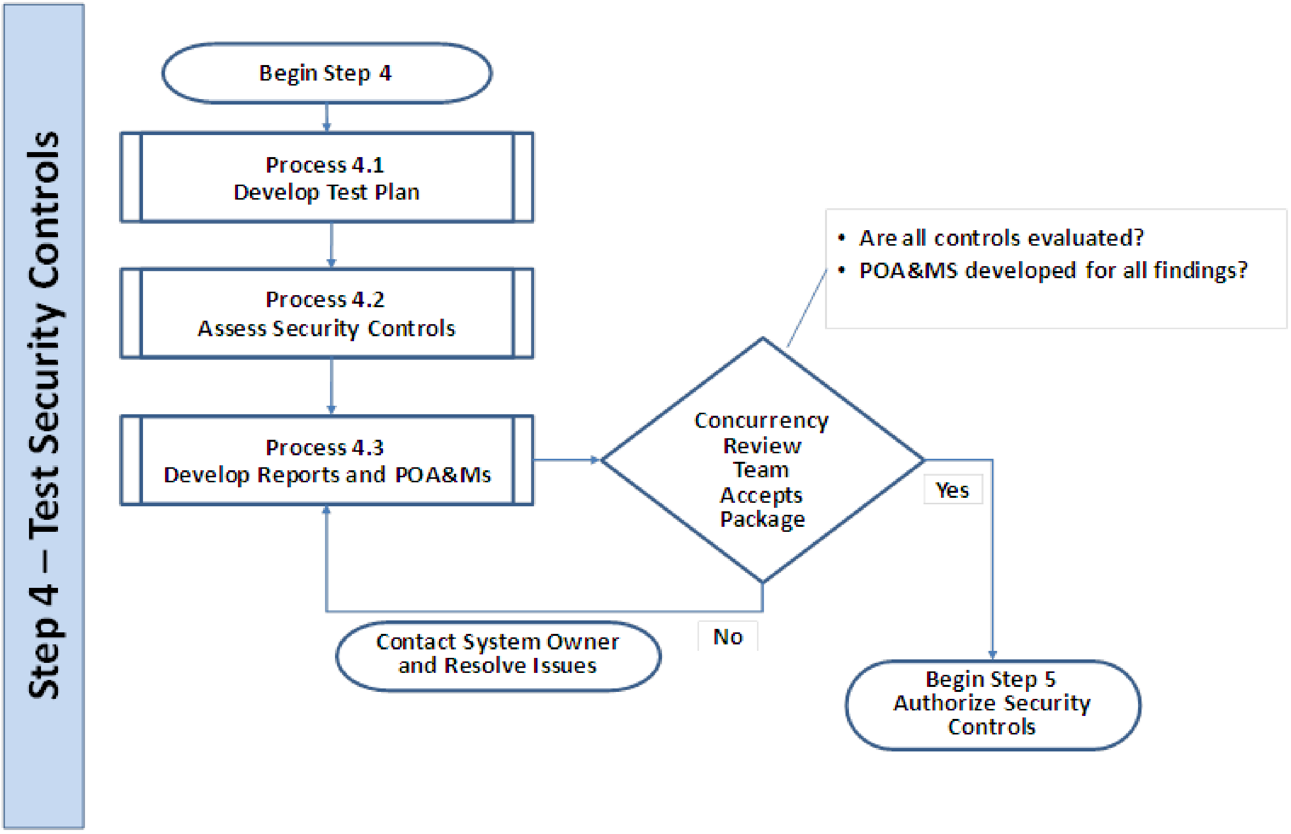

Step 4 – Test Security Controls
Begin Step 4
Process 4.1
Develop Test Plan
Process 4.2
Assess Security Controls
Process 4.3
Develop Reports and POA&Ms
Concurrency Review Team Accepts Package
• Are all controls evaluated?
• POA&MS developed for all findings?
Yes
No
Contact System Owner and Resolve Issues
Begin Step 5
Authorize Security Controls

Figure 2-4: RMF Step 4 - Assess Security Controls

2.5.1 Develop a Security Assessment Plan

At the start of testing, the independent assessor (for moderate/high systems) will create a security assessment plan. A template of this plan can be found in Appendix B. This plan will define the boundaries of the system, the testing methodologies, a description of any sampling that was done, and provide a general guide to the testing of the system. The assessment must be performed on all components of the system as defined in the SSP. An important aspect of this is the tests that will be accomplished. For this, the assessor utilizes a blank CSAM security assessment report that is generated for the system by CSAM. This is done from within CSAM by selecting "Assessments" – "Assessment Reports/Views" - and then "Security Assessment Template". For the sub-heading "Applicability" select "Applicable" and run the report, when complete, select "Hybrid" and run the report again. CSAM does not currently add the hybrid controls to the "Applicable" selection so two reports must be run to see all the tests that must be accomplished (DOJ developers are working to fix this). The blank report provides the perfect medium for the tester to complete the security controls assessment. The report contains the control implementations and the tests that need to be performed. This method simplifies the act of entering the test results for each test back into CSAM. Once the results are entered, a Plan of Action and Milestones (POA&M) can be generated by CSAM to document security deficiencies. If the System Owner performs any remediation to reduce risk, a retest of those controls is initiated and the results entered directly into CSAM.

2.5.2 Perform the Security Controls Assessment

Using the blank security assessment report generated under Section 2.5.1 as a guide, the assessor must interview, examine, and/or test the applicable security controls. This includes gathering evidence for the tested controls and documenting the results within the security assessment report. Note that each test requires evidence of test compliance or non-compliance. This evidence must be specific in nature and support the testing that was done. Examples of evidence can be an interview (with interviewee name, date, and time of interview documented), a test (screen shots and/or portions of a file to be included) or a document (including the document's formal name, version, and date) or a combination of the above.

The assessor must also perform a vulnerability scan of the components comprising the system and analyze and summarize the results of the scan. If the system/application is hosted at a data center or on a GSS, then the assessor may utilize the results of the most recent scan provided by the GSS central scanners.

If possible, the assessor performs a compliance scan of the components comprising the system with a scanner capable of utilizing the XCCDF and OVAL test file downloaded from the NIST USGCB site. The assessor must summarize the results, highlighting high/moderate risk items, and identify the percentage of system compliance to the required baseline(s).

Reuse of Evidence

In keeping with NIST requirements to minimize the costs of testing, assessors can reuse evidence from the last test that was accomplished on the system as long as the testing was not done longer than six (6) months prior to the current test date. The reused evidence must be handled following the same guidelines as any new evidence gathered in support of a test.

Large System Testing/Sampling Techniques

Occasionally, very large and complex systems will need to undergo a security control assessment. For large systems, device/component sampling is the accepted means of performing the assessment. Sampling shall be done in accordance with the following:

- Sampling will only be done for specific types of devices when there is a quantity of 26 or more.
- Sampling for these types of devices will be performed by taking a random selection of the devices to achieve a total of at least 10% of the initial quantity (a minimum of 10 devices will be tested).

Types of devices can be determined by the make and model, the function, and/or the operating system.

Example 1:

System: A system includes 100 desktop computers, all running Windows XP.

Testing: 10 desktops will be tested.

Rationale: 10 % of the initial quantity of 100 equals 10. 10 is also the minimum number of devices that will be tested. It does not matter what make or model the desktop computers are.

Example 2:

System: A system includes 25 Windows Vista desktops and 75 Windows XP desktops.

Testing: 25 Windows Vista desktops and 10 Windows XP desktops will be tested.

Rationale: The number of Windows Vista desktops is below the threshold of 26 needed before sampling can be used. Therefore all 25 must be tested. The number of Windows XP desktops is greater than 26, so sampling is allowed. A 10% sampling of 75 desktops would yield a total of 8 machines to be tested. This is below the minimum number of 10 devices that must be sampled, so a minimum of 10 Windows XP desktops must be tested.

Example 3:

System: A system includes 50 routers; 30 of them are Cisco and 20 are Enterasys.

Testing: 10 Cisco and 20 Enterasys routers will be tested.

Rationale: 30 routers is greater than the number needed to perform sampling. 10% sampling for a sample of 30 would yield a total of 3 machines tested. This is below the minimum number of 10 devices that must be sampled, so 10 Cisco routers will be tested. 20 Enterasys routers is below the threshold needed before sampling can be used. Therefore, all 20 Enterasys routers will be tested.

Example 4:

System: A system consists of 50 servers: 3 are domain name servers, 4 are Microsoft Exchange servers, 5 are database servers, 25 are file servers and 13 are FTP servers.

Testing: All 50 servers will be tested.

Rationale: Though 50 servers are above the threshold needed for sampling, each of the types/uses of the servers are different from the others. Of the types of servers in the system, none has a quantity exceeding the threshold of 26. Therefore, all servers will be tested.

The sampling technique and listing of actual equipment tested shall be included in the Security Assessment Plan.

Enter Results of the assessment into CSAM

In CSAM, the assessor or designated representative should open each control for the system and input the individual results for all of the tests for that control. The results should be specific to the system and directly address the test that was performed. These tests have also taken on the name "Determine If statements" because most tests start with the phrase "Determine If..."

The assessor should mark whether the test/Determine If is:

- Not Assessed (Test/Determine If was not tested). This option should never be checked. All tests must be addressed for the assessment to be complete.
- Satisfied (Results satisfy the test/Determine If statement).
- Other than Satisfied (Results do not fully satisfy the test/Determine If statement.)
- N/A (Test/Determine If is not applicable to the system).

The assessor will enter the date of testing. The first line of every test result should identify the date and time of testing.

The assessor will enter the results from the testing into the "Assessment" - Assessment Search" section of CSAM. This section will detail the exact results of the testing. Be sure that all responses that are entered within the "Finding" section address the appropriate Determine If statement.

The assessor should enter the methods used to assess this control within the "Methods and Objectives" section in CSAM. This section should detail the documents that were examined ("We examined USDA Contingency Plan version 2.1, dated 11-13-10"); people that were interviewed along with their title and contact information and date and time ("We interviewed system administrator Mark Whitten (mark.whitten@usda.gov) on 11-15-10 at 10:15am in his office-Rm. 435W"), and screenshots of items that were tested ("We tested password masking; the screenshot can be found in "*FY13 <System> A&A Evidence.zip*.".)

Each test result must be specific to the system tested and specifically answer the "Determine If" statement. Each test result must also be supported by evidence that helps to prove or justify the result. The test evidence must be documented, specific in nature, and support the testing that was done. Evidence can be an interview (interviewee name, date, and time of interview must be included), a test (screen shot, portion of a file must be included) or a document (formal name, version, date must be included) or a combination of the above. All evidence used to support testing becomes part of the test record and must be attached/uploaded to CSAM. When documenting system testing, open a testing zip file with the name "*FY13 System A&A Evidence.zip*" and work through the tests of the security assessment report putting all evidence into the zip file. The results for each test must include a statement that points to the file name(s) for where that evidence can be found in CSAM. This pointer statement would look like the following "This evidence can be found in "*FY13 System A&A Evidence.zip*".

Although CSAM was designed to link test evidence to each test, do not link any tests to the uploaded evidence files. Simply refer to the file name of the zip file within the test result statement as described above.

Example: On 10-12-12 at 10:00 AM, we examined *XYZ System Contingency Plan* version 2.1 dated 11-13-10. This document can be found in "*FY11 System A&A Evidence.zip*".

> When the reviewer looks at Appendix F of CSAM and finds "*FY11 System A&A Evidence.zip*" file; when opened, the document "*XYZ System Contingency Plan*" should be easy to find.

The SSP should seldom be attached as evidence. There are some specific Determine If statements that ask specific questions about the security plan and there are others that look for a "defining statement" of agency/system policy. In these cases, the security plan can be listed as evidence and there is no requirement to upload the security plan as an artifact. In cases where an interview is the only evidence, there is no requirement for an uploaded artifact as long as the interview is properly documented as described above. Do not upload evidence that does not support the specific test. Uploading test results or an interview for a Determine If statement that is looking for where something is defined and what is defined is incorrect.

When testing results have been completed and entered into CSAM, every test should contain:

- Date and time of when the test was accomplished;
- Identify who conducted the testing;
- Statement(s) that describe the results of the specific “Determine If” tests as they relate to the specific system;
- Evidence that specifically supports the statement(s) made; and
- A pointing statement that directs the reader to the file name of the evidence.

The testing evidence zip file should be placed in CSAM Appendix F. The appendix should have the name: “**FY13 A&A Assessment Evidence**”

2.5.3 Develop/Review Security Assessment Report, Risk Assessment and POA&Ms

When the testing is complete, there are a number of steps that need to be accomplished in CSAM to ensure that results are entered correctly:

- For each control that has failed, generate a POA&M entry;
- Identify to whom the POA&M is assigned;
- Generate the Security Assessment Report and verify that there are no tests listed as "Not Assessed";
- Generate the Security Assessment Report and verify that every test listed as "NA" has a valid reason for being not applicable and is supported by evidence;
- Generate the Risk Assessment Report "Risk Analysis" and post this report to CSAM Appendix G2;
- Generate the Risk Assessment Report "Threat Matrix" and post this report to CSAM Appendix G3;
- Generate the Risk Assessment Report "Residual Risk Report". Verify that every residual risk identified can be traced back to a POA&M. If not, then a POA&M must be created for the identified vulnerability. Once this is completed, generate another "Residual Risk Report" and post this report to CSAM Appendix G4;
- Ensure that all POA&Ms are approved; and
- Ensure the evidence file has been uploaded into Appendix F: “FY13 A&A Assessment Evidence”.

2.5.4 Risk Based Decisions (RBD)

To some degree, risk is always present in an operational system. The issue(s) causing the risk is either mitigated, and thereby the risk reduced, or accepted and it remains. The decision to operate a system is an example of a risk based decision as frequently not all the controls are in place. This section presents a method to deal with system specific vulnerabilities and the risk associated with them. There are instances a system and/or program vulnerability, due to the resource expense, cannot be corrected. These decisions can only be made after a thorough evaluation of the risk and the resources required to correct or minimize that risk.

Vulnerabilities must be evaluated to determine the effect they may have on both the agency environment and the USDA IT enterprise, taking into consideration RBDs and existing POA&Ms from other interconnected and/or hosted systems. Vulnerabilities that are candidates for risk based decisions must be evaluated by the agency and then forwarded to ASOC OCD for evaluation and potential escalation to the USDA CISO for concurrence. All vulnerabilities that are considered for a RBD must be forwarded to ASOC OCD. If ASOC OCD concurs with the agency's decision to issue an RBD, it may then be sent to the system AO for signature. The RBD is documented, by the agency, in a memo from the system AO to the System Owner who will then modify the system/program security plan documenting the vulnerability as a risk based decision in CSAM. The System Owner can also close any POA&Ms that existed for the identified vulnerability but the RBD's will be reported annually for re-evaluation and renewal.

An RBD may not be utilized as an interim authority to operate (IATO) mechanism or used to relieve the System Owner of implementing items that are mandatory (Executive Orders, baseline and/or critical operational security requirements, vulnerability scanning or remediation, etc.)

The following actions will be elevated from ASOC OCD to the USDA CISO for evaluation and approval before implementation:

- RBD of inheritable control(s) provided by a data center or GSS;
- RBD of identification, authorization or access control mechanisms of a system;
- RBD of scanning mechanism(s) and/or deviation from the configuration management baselines set by ASOC;
- RBD that involves more than one agency; and
- RBD that could affect the overall security of USDA.

RBDs will be tracked, reviewed annually by the System Owner, and forwarded to the AO for approval on a yearly basis. Since the assignment of risk can change over time, the RBD will also be forwarded to OCD for review and concurrence on an annual basis. Note this should be done collectively for all their systems at the same time.

OCD will generate periodic CSAM reports of RBDs and outstanding POA&Ms for each system for evaluation at the overall Departmental level.

For detailed RBD procedures for processing RBDs refer to the POA&M SOP.

2.5.5 Step 4 Completion Summary

- Develop Security Assessment Plan. Post it to Appendix E.

- Security controls assessment performed.
- Test results entered into CSAM.
- Verify that there are no "Not Assessed" tests in the Security Assessment Report.
- Verify that every test of the Security Assessment Report that is marked as "NA" has a valid reason for being not applicable and is supported by evidence.
- Verify that every test has detailed evidence listed.
- Generate the CSAM risk reports and post them to Appendices G-2 (Risk Assessment Results), G-3 (Risk Threat Pairing), and G-4 (Residual Risk Report).
- Verify the evidence file has been uploaded into Appendix F: “FY13 A&A Assessment Evidence”
- Program/system notification submitted via email to the Cyber Communication mailbox (Cyber.Communication@usda.gov) requesting Step 4 Concurrency Review.

2.6 Step 4b: Submit the Package for Final Concurrency Review

The system owner/ISSPM/CISO sends an email to the concurrency review team at Cyber.Communication@usda.gov stating the package is ready for review in CSAM. The concurrency review team will review the system’s Step 4 documentation against the concurrency review checklists for compliance with NIST and Departmental standards. This concurrency review covers all A&A package documents. At the conclusion of the concurrency review process, the System Owner/Authorizing Official will receive either a concur memorandum from OCD with a recommendation to proceed to authorization or one or more checklists listing items that must be remediated and re-reviewed prior to the issuance of a concur memorandum. The checklists utilized in concurrency review are located in Appendix C.

Below is checklist with the items to be completed for step 4:

- Program/system notification submitted via email to the Cyber Communication mailbox for Step 4 concurrency review.
- Concurrency review Step 4 comments received via completed checklists.
- Update assessment and POA&M results in CSAM based on concurrency review comments.
- Program/system re-submitted via email to the Cyber Communication mailbox for Step 4 concurrency re-review.
- Program/system concur memorandum received by agency from OCIO OCD.
- Concur memorandum uploaded to the ”Security Authorization” section of the CSAM status page and then post to Appendix H.
- Concurrency review will generate the Security Assessment Report and the Residual Risk Report and post them to the Appendices F*x* and F*x* with titles “FY13 A&A

Security Assessment Report" and "FY13 A&A Residual Risk Report". "x" means the next consecutive numbered "F" appendix. (This is the A&A archive copy).

- Concurrency review will create a zip file of all review checklists and post it to Appendices Fx with titles "FY13 A&A Concurrency Review Checklists". "x" means the next consecutive numbered "F" appendix. (This is the A&A archive copy)

2.6.1 Authority to Test

In the course of performing security controls testing for a new system, there may be a need for the system to actually be in production for a short period of time to allow accurate and worthwhile testing to be accomplished. All effort should be made to test this system in a pre-production environment, but should that not be feasible, an Authority to Test may be granted by the ACIO, OCD. Such authority will only be granted after the satisfactory completion of the Step 3 concurrency review and will only be in effect through the completion of testing, at which time the system will be removed from operation until the Authority to Operate is granted.

2.7 Step 5: Authorize Information System

During Step 5, the required evidence is produced to provide the AO with the information needed to make an informed risk based decision. The residual risk report documents the risk determined for the vulnerabilities found during assessment of the security controls. The subsequent POA&Ms include costs and remediation plans.

Tasks Performed by System Owner (SO)	Authorizing Official (AO)
• Remediate AO identified issues if necessary to achieve ATO • E-mail ATO letter to Cyber.CSAM@ocio.usda.gov and request to update the restricted ATO field in CSAM	• Review/validate risk, POA&M and ATO constraints with System Owner • Generate authorization recommendation or denial with System owner involvement

During authorization, the certification agent or ISSPM gathers the key A&A package documents (Step 4 concur memorandum, POA&M, Security Assessment Report, and SSP) for the AO/DAA to make a decision concerning the authority to operate (ATO). The AO/DAA weighs any remaining vulnerabilities and risks of system operation and then determines what residual risk to accept, what remedial actions are required (i.e., POA&Ms), and whether or not to issue an ATO.

Below is the overall process for RMF Step 5.

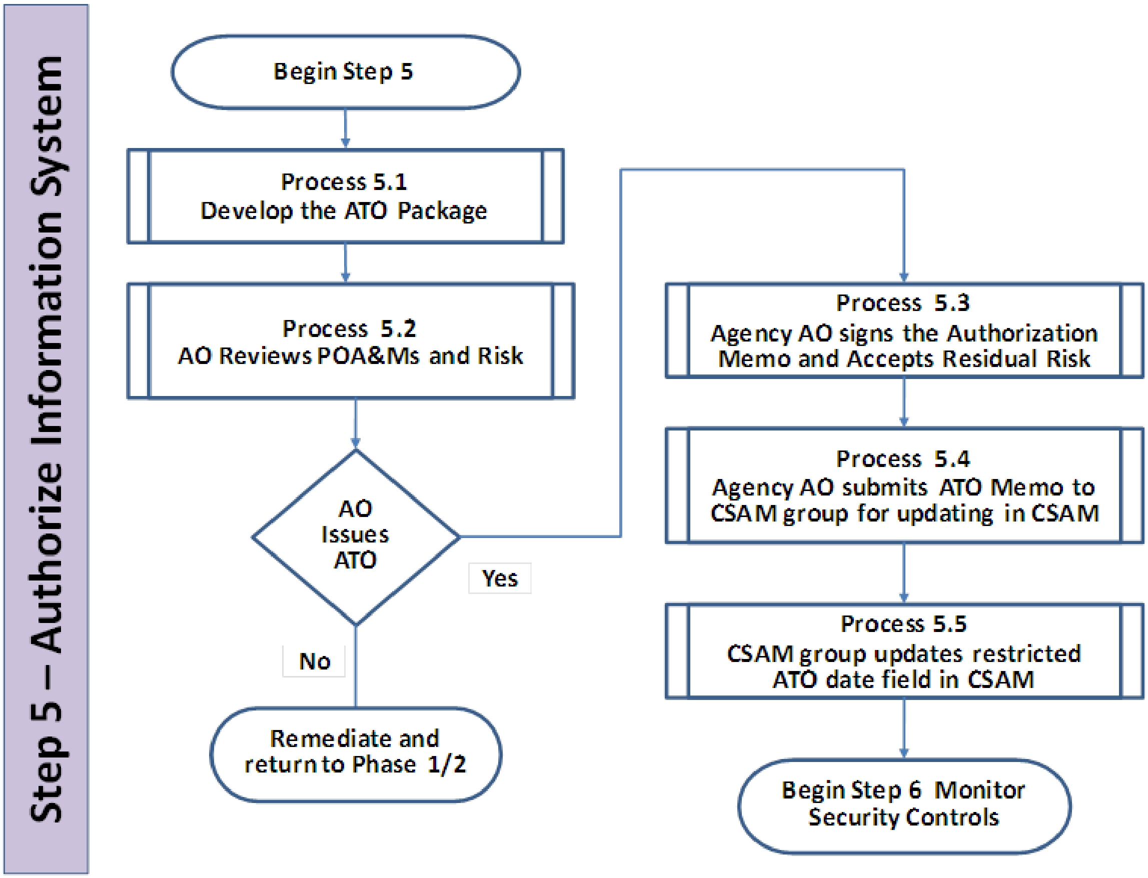

Step 5 – Authorize Information System
Begin Step 5
Process 5.1
Develop the ATO Package
Process 5.2
AO Reviews POA&Ms and Risk
AO Issues ATO
Yes
No
Remediate and return to Phase 1/2
Process 5.3
Agency AO signs the Authorization Memo and Accepts Residual Risk
Process 5.4
Agency AO submits ATO Memo to CSAM group for updating in CSAM
Process 5.5
CSAM group updates restricted ATO date field in CSAM
Begin Step 6 Monitor Security Controls

Figure 2-5: RMF Step 5 - Authorize Security Controls

If the AO denies authorization to operate, s/he meets with the System Owner and agency CIO, along with an OCIO ASOC representative to develop a strategy for remediation or remove the system from the network.

Once the Program/system ATO is signed, it must be posted in CSAM via the status page to "Security Authorization" and then to Appendix R. An email must be sent to the Cyber CSAM mailbox (cyber.csam@usda.gov) stating that the ATO has been posted in CSAM. The CSAM Administrator will verify the document has been posted and will update the ATO date for the system.

Below is a checklist for Step 5 Authorize security controls:

- Assemble ATO package for presentation to AO.
- Program/system ATO signed by AO.
- Program/system Concur Memorandum from ASOC OCD posted to the CSAM Status Page to Security Authorization section and then post to Appendix H.
- Program/system ATO posted through the CSAM Status Page to Security Authorization section and post to Appendix R.

- Send email to Cyber CSAM that the ATO is posted in CSAM and request the ATO status and date be updated.
- Verify that the ATO date has been updated on the CSAM status page for that system by the Cyber CSAM group.

2.8 Step 6: Monitor Security Controls

Once the system is authorized for operation, it is ready to enter the continuous monitoring phase. Continuous monitoring consists of three tasks: (1) configuration management and control; (2) security control monitoring; and (3) status reporting and documentation. The purpose of this step is to provide oversight and monitoring of the security controls in the information system on an ongoing basis and to inform the AO when changes occur that may impact the security of the system. Continuous monitoring activities ensure that secure system management, operation, and maintenance preserve an acceptable level of residual risk. ***The activities in this step are performed continuously throughout the life cycle of the information system.***

Tasks Performed by System Owner (SO)	Authorizing Official (AO)
• Review system changes and start re-accreditation if major change occurs • Remediate POA&Ms • Document updates to SSP, CP, CMP, IRP • Continual scanning of information systems for vulnerabilities • Review the system and complete the "System Annual Review Memo" found in Appendix B of this document annually.	• Review/validate risk, POA&M, system changes, and documentation with System Owner annually

Table 2 –1 Annual Monitoring Tasks

2.8.1 Continuous Monitoring Process Overview

Below is the overall process for RMF Step 6.

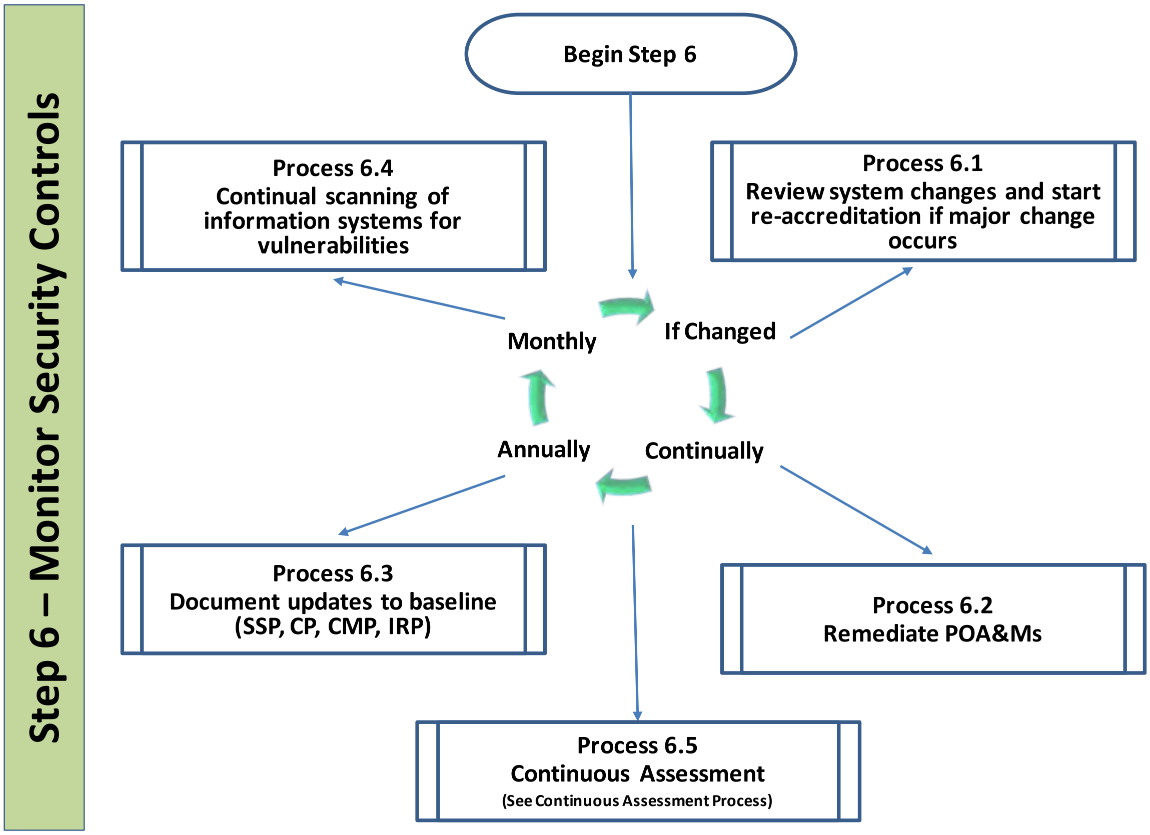

Step 6 – Monitor Security Controls
Begin Step 6
Process 6.4
Continual scanning of information systems for vulnerabilities
Process 6.1
Review system changes and start re-accreditation if major change occurs
Monthly
If Changed
Annually
Continually
Process 6.3
Document updates to baseline (SSP, CP, CMP, IRP)
Process 6.2
Remediate POA&Ms
Process 6.5
Continuous Assessment
(See Continuous Assessment Process)

Figure 2-6: RMF Step 6 - Monitor Security Controls

During this step, the ongoing activities of continuous scanning of technical controls and monitoring of other selected management/operational controls on a monthly/annual basis are accomplished. Updates to documentation, remediation and closure of POA&M(s) in CSAM as required are also performed during this step of the NIST RMF process. The set of controls assessed each fiscal year was formalized by a departmental working group which issues updates on an annual basis and organizes them into groups within CSAM to facilitate department wide reporting. Once the results for each system are uploaded to CSAM, they are inspected each year by concurrency review.

The controls to assess annually (both Key and annual control sets) as defined by the department are located in appendix E of this guide. This list is officially disbursed annually via a departmental memo and also posted, with updates to this guide, on the departments OCIO Cyber web site at:
http://www.ocionet.usda.gov/wps/portal/ocio/ocioportal/home/security/security_ca

This process replaces the prior annual controls assessment procedures and is depicted below:

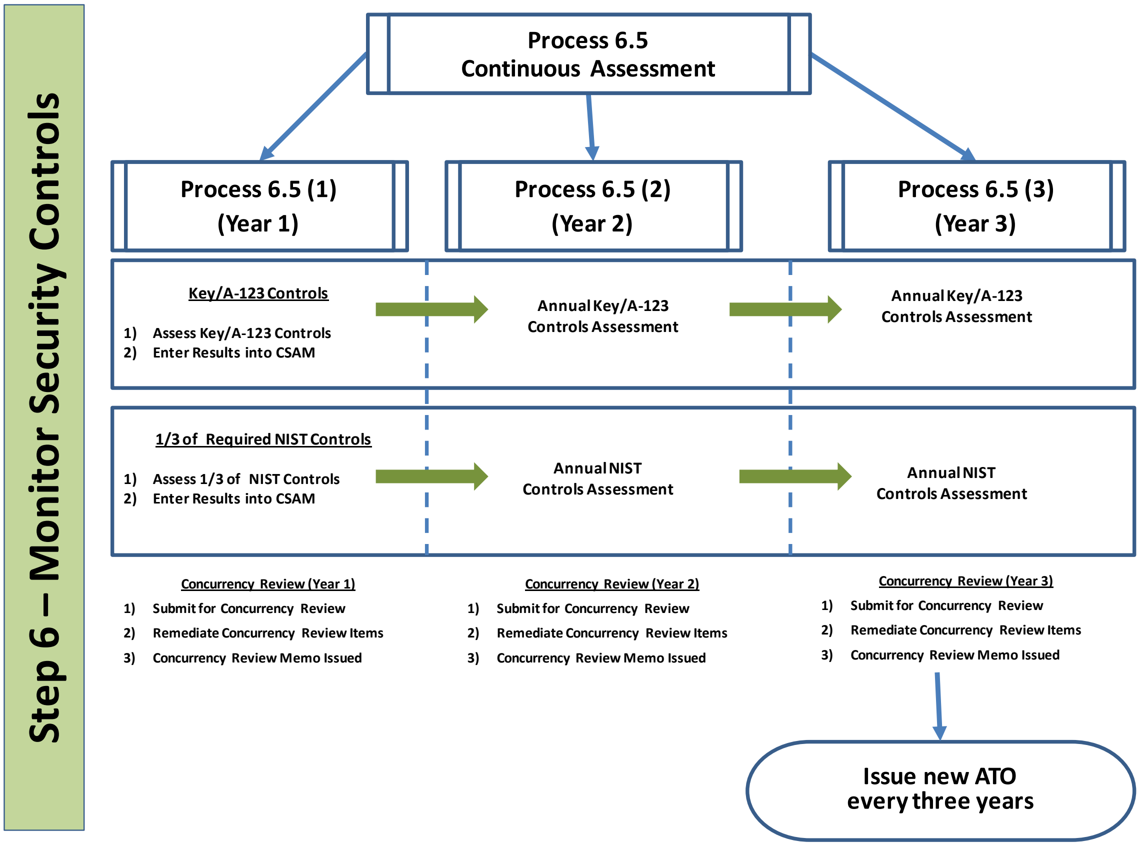

Step 6 – Monitor Security Controls
Process 6.5
Continuous Assessment
Process 6.5 (1)
(Year 1)
Process 6.5 (2)
(Year 2)
Process 6.5 (3)
(Year 3)
Key/A-123 Controls
1) Assess Key/A-123 Controls
2) Enter Results into CSAM
Annual Key/A-123
Controls Assessment
Annual Key/A-123
Controls Assessment
1/3 of Required NIST Controls
1) Assess 1/3 of NIST Controls
2) Enter Results into CSAM
Annual NIST
Controls Assessment
Annual NIST
Controls Assessment
Concurrency Review (Year 1)
1) Submit for Concurrency Review
2) Remediate Concurrency Review Items
3) Concurrency Review Memo Issued
Concurrency Review (Year 2)
1) Submit for Concurrency Review
2) Remediate Concurrency Review Items
3) Concurrency Review Memo Issued
Concurrency Review (Year 3)
1) Submit for Concurrency Review
2) Remediate Concurrency Review Items
3) Concurrency Review Memo Issued
Issue new ATO
every three years

Figure 2-7: Continuous Assessment and Authorization Tasks

Below is the checklist for Step 6, Monitor Security Controls.

- Validate that the vulnerability scanning is being accomplished and configuration management issues remediated in a timely fashion.
- Validate that progress is being made on POA&Ms items and milestones are updated in CSAM.
- Validate that key controls and the set of controls defined for assessment in that fiscal year are tested annually (reference Appendix E for the sets of controls to assess).
- After annual testing, generate the CSAM risk reports and post them to Appendices G-2 (Risk Assessment Results), G-3 (Risk Threat Pairing), and G4 (Residual Risk Report).
- Annually complete the “System Annual Review Memo” found in Appendix B - Templates to this document. Post this memo in accordance with the instructions on the memo.

2.8.2 Significant (Major) Change Definition

For the purposes of continuous monitoring, the definition of a major change, also known as a significant change, is key to determining if some or all or the controls need retested.

In an effort to help system owners and managers understand what constitutes a significant change to USDA systems, we have provided some representative examples below that would require a system to be re-certified/ re-accredited or to perform a targeted assessment. These examples are not a definitive list of conditions that may exist, but have been provided to demonstrate many of the common situations that Authorizing Officials and System Owners may encounter and need to address.

A significant change alters the mission, operating environment, or security state of a system. Examples of significant change include: increase/decrease/upgrades in hardware, change in application programs, change to operating system (including version upgrades), addition of external users when previously there were no external users, additions of telecommunications capability, changes to the program logic of application systems, or relocation of the system to a new physical environment or new organization.

Examples of changes that require a full A&A:

- Changes that involve/impact Privacy Act data;
- Changes in a system’s sensitivity or classification level;
- Changes in sensitivity or classification level of data being processed; or
- An incident that results in a breach to an information system, producing a loss of confidence by the organization in the confidentiality, integrity, or availability of information processed, stored, or transmitted by the system.

Examples of changes that would require a targeted security assessment (a targeted assessment is the retesting of all controls that were affected due to the change):

- Changes to accreditation boundaries;
- Adding an interconnection to a system with a different Authorizing Official;
- Relocation to a different site/facility;
- Outsourcing management of a system;
- Adding a public facing component to the system;
- Rewrite/recoding of a system/subsystem/module using new technology;
- Adding or activating a new subsystem/module to a system or subsystem;
- Deleting a subsystem/module that affects the security of the parent;
- Findings from a review that identifies un-assessed risk;
- Changing user authorization mechanisms (e.g., changing from an application-specific authorization to active directory, eAuthentication, or other access technology);
- Hardware changes/upgrades;
- Operating system version changes/upgrades (e.g., Windows 2000 to Windows Server 2003);
- Operating system conversion (e.g., Windows 2000 to Unix); or
- Application changes/upgrades (e.g., SQL 2000 to SQL 2007).

Moving systems or child systems from one place in CSAM to place them under another system (as a child) or to make them a separate system in CSAM is considered a major change.

You are in effect changing the boundaries of one or more systems and this type of move cannot be made without looking at the ramifications to the certification of all systems involved. Children/systems will not be moved if their ATOs are within 6 months (unless approved by the COE) of expiring unless the parent system that will ultimately contain the moved system also has an ATO that is within 6 months of expiring. Agencies desiring to move systems in CSAM must submit a memo to OCD at cyber.communication@usda.gov requesting the CSAM move. The memo must detail the actions that will be accomplished by the move and specify the proposed ATO dates of the systems involved (if applicable). Due to potential issues associated with parent/child reorganizations, it is strongly suggested that the OCD concurrency review team and agency COE liaison be consulted prior to moving any systems to ensure the changes comply with NIST and USDA guidelines and requirements.

For targeted assessment decisions, the system's Authorizing Official must work in consultation with the Department's risk executive (function), system and mission/business owners, the agency's senior information security officer, and the agency CIO to ensure the decision does not have an effect on systems outside of the system/application boundary.

For systems undergoing a targeted assessment on an existing system, a new authorization to operate (ATO) memorandum would be required once the assessment was complete. The ATO date on the new memo would be the same as the original ATO memo.

Recording in CSAM, the system is undergoing modification.

Major changes, just like other changes, should be accomplished off-line (test environment) and then tested prior to being placed into production as directed by the NIST SP800-53 Configuration Management family of controls. This testing does not remove the requirement to re-test the actual production system, either before the system is placed back into production or after the change has been made and the system is in production. It should be noted that as soon as you commence changing the system, you invalidate the current ATO and you are operating the system at risk until the system once again completes Step 3, 4 and 5 of this guide. To ensure that this change is properly documented, as soon as a major change is made to a system, the System Owner is required to send an email to cyber.communication@usda.gov and inform OCD of the major change. At that time, CSAM will be updated to indicate that the system is in modification status indicating that the systems is operational but undergoing a major modification.

Defining and addressing significant change can at times seem to be more art than science. If agencies have questions or are unsure if they have a condition that would warrant either a full or targeted security assessment, they should contact ASOC at cyber.communication@usda.gov.

2.8.3 Transition to Continuous Assessment and Authorization

USDA is starting the migration to continuous assessment/continuous monitoring under NIST 800-37 Revision 1. Any system(s) that fall under the following criteria must traverse the normal six step NIST/USDA RMF process before being authorized/re-authorized (See Section 2.1).

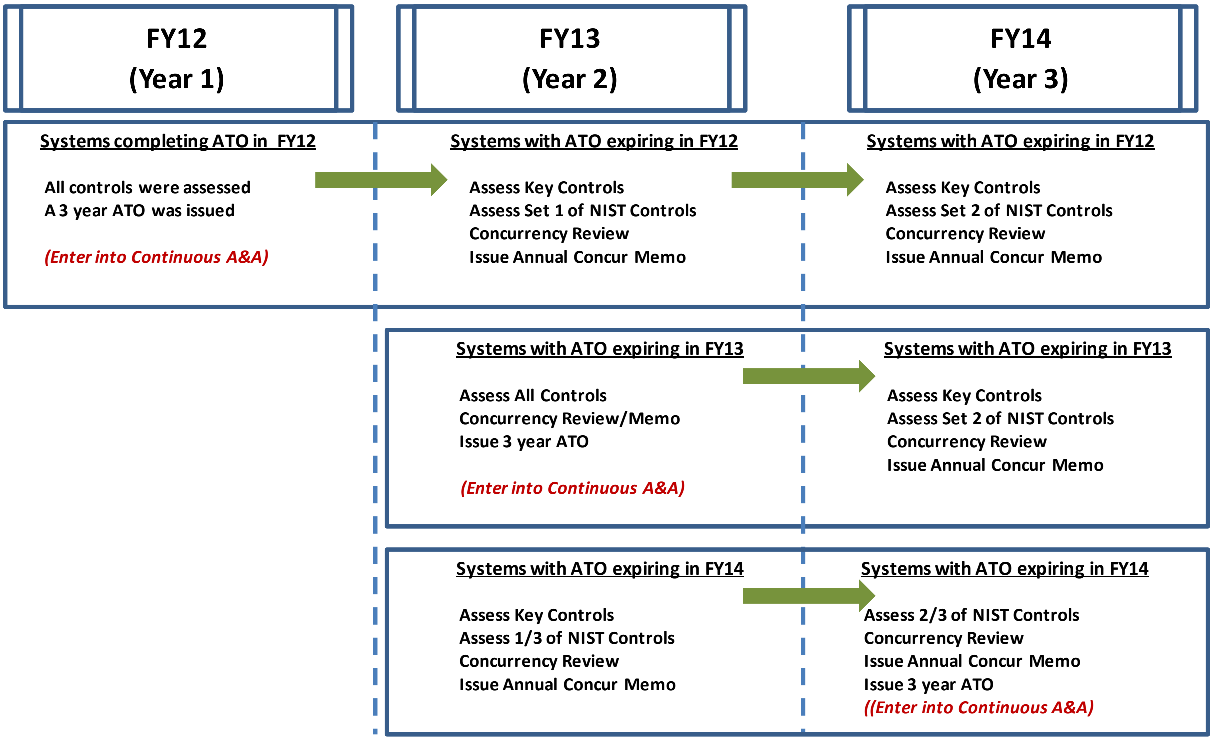
- Systems with an ATO that expires on or before FY13.
- New Systems that do not have a current ATO.

- Systems that have undergone a major change.

Systems with an ATO that expires in FY 2014 and FY 2015 shall follow the procedures below.

Per NIST 800-53 Revision 1, all controls must be assessed during the three year ATO cycle. Implementation of continuous monitoring, as defined in this document, should reduce system security management costs and leverage annual testing requirements to apply toward the system's authorization requirements. Systems and programs will still be formally approved for operation (Authority to Operate) every 3 years; however, control testing will be spread out over the 3 year accreditation period, testing 1/3 of the NIST controls annually.

To ensure consistency across USDA, the Department will specify the controls that will be tested annually. The initial list of controls to be tested annually can be found in Appendix B and the FISMA Key controls can be found in Appendix C of this document. Adjustments to these control sets will be issued at the start of every fiscal year (i.e., the key controls may change, the one-third of annual NIST controls may not). The implementation of continuous assessment/continuous monitoring will be as follows:



FY12 (Year 1)	FY13 (Year 2)	FY14 (Year 3)
<u>Systems completing ATO in FY12</u> All controls were assessed A 3 year ATO was issued *(Enter into Continuous A&A)*	<u>Systems with ATO expiring in FY12</u> Assess Key Controls Assess Set 1 of NIST Controls Concurrency Review Issue Annual Concur Memo	<u>Systems with ATO expiring in FY12</u> Assess Key Controls Assess Set 2 of NIST Controls Concurrency Review Issue Annual Concur Memo
	<u>Systems with ATO expiring in FY13</u> Assess All Controls Concurrency Review/Memo Issue 3 year ATO *(Enter into Continuous A&A)*	<u>Systems with ATO expiring in FY13</u> Assess Key Controls Assess Set 2 of NIST Controls Concurrency Review Issue Annual Concur Memo
	<u>Systems with ATO expiring in FY14</u> Assess Key Controls Assess 1/3 of NIST Controls Concurrency Review Issue Annual Concur Memo	<u>Systems with ATO expiring in FY14</u> Assess 2/3 of NIST Controls Concurrency Review Issue Annual Concur Memo Issue 3 year ATO *((Enter into Continuous A&A)*

Figure 2-8: Transition into Continuous Assessment/Authorization

2.8.4 Continuous Assessment/Continuous Monitoring Process

The continuous Assessment/continuous Monitoring process may seem like a big change in the way that a system in the RMF process maintains its ATO. The changes are mainly the elimination of the complete re-testing of all controls at a single time during the 3 year period.

Changes to other existing tasks are actually minimal, other than the switch to an annual concurrency review. The process is explained below:

System/Program Annual Review:
The system/program owner performs the annual documentation review/update for each system/program:

- System/Program Security Plan (including updating these sections)
  - Points of contact
  - Connections to other systems (i.e. ISAs, MOUs, MOA, SLAs)
  - Steps and permissions required to access the system (i.e. access path)
  - Auditing information
  - Categorization
  - Hardware/Software Inventories
  - Privacy Threshold Analysis/Privacy Impact Analysis
  - Designated annual controls (controls designated by OCD)
  - Key controls (controls designated by OCD)
- Contingency/Disaster Recovery Plan
- Contingency/Disaster Recovery Test – Accomplished
- Contingency/Disaster Recovery Test – Reviewed
- Configuration Management Plan (Required at least every three years)
- Incident Response Plan (Required at least every three years)

Concurrency Review (RMF Step 3b)
Following the procedures under Section 2.4, submit the system/program for an RMF Step 3b concurrency review. The concurrency review will focus on the SSP with specific attention to the key and designated annual controls and what may have changed.

Assess Security Controls (RMF Step 4a)
Following the procedures under Section 2.5, perform the RMF Step 4a system/program assessment, but only test the key and designated annual controls.

Concurrency Review (RMF Step 4b)
Following the procedures under Section 2.6, submit the system/program for an RMF Step 4b concurrency review. The concurrency review will focus on all documentation with specific attention to the testing of the key and designated annual controls.

Upon completion of the RMF Step 4b concurrency review, the agency will receive a concur memo for that years continuous monitoring controls assessment. Should the system/program ATO expire that year, a concur memo for that ATO will be issued, please follow the procedures under Section 2.7 and continue working within the framework of Section 2.8. If the system/program ATO does not expire that year, continue working within the framework of Section 2.8. If the ATO expires that year then an ATO may be re-issued once you receive a concur memo for the 3rd year.

2.8.5 Clearing POA&Ms and Updating the Risk Assessment

When a residual risk report is generated in CSAM, CSAM pulls in all failures from controls inherited (hybrid) from other systems in CSAM. Therefore a test failure from one system can and will show up in the residual risk report for a number of other systems if the control that failed is designated as a common/hybrid control. This new CSAM feature makes it even more important that POA&Ms are properly cleared and the CSAM risk assessment updated. All POA&Ms must be associated with a NIST 800-53 control. This allows a more comprehensive testing sequence to be performed to ensure that the vulnerability has indeed been corrected/mitigated.

Once all the actions have been taken to correct the vulnerability that is documented by a POA&M, you must demonstrate that the vulnerability has indeed been corrected. This is especially important when the POA&M is the result of a failed test during a system assessment. When an assessment test fails, it is documented in the security assessment report and then it shows up in the residual risk report where it is associated with a POA&M.
Since all POA&Ms are associated to a control, to clear a POA&M, the NIST 53A tests that have been identified for that control must be re-performed with the test results documented in CSAM using the same documentation requirements used for an assessment. These are:

- The test results must address the test
- Every test must be supported by evidence
- The evidence must be clearly identified and easily found in CSAM.

Test evidence for the clearing of POA&Ms is treated differently than evidence for assessments. Evidence for re-testing a specific control (clearing a POA&M) will be placed in a zip file with the name “Evidence [Control Family] – [Control Number] [date]”. This ZIP file will be placed into another zip file titled “[System Name] POA&M Closure Evidence” which will be placed in CSAM Appendix P. CSAM Appendix P will be the appendix that houses all POA&M closure evidence. The evidence will all be in one zip file that contains a zip file for every control tested.

Once the tests are completed, the residual risk report is generated in CSAM and (assuming that all the tests passed) posted to CSAM Appendix G4.

For detailed procedures POA&M management, please refer to the POA&M guide.

3 A&A Documents, Processes and Information

This section includes a brief description of the documents and processes needed to complete the A&A process at USDA. Because USDA fully utilizes the capabilities of CSAM, some documents that used to be created outside of the system are either no longer needed because CSAM generates them or they have been retired from use.

3.1 CSAM Appendices and the CSAM Status Page

The CSAM status page provides the reader with a quick view of the status of the system. In addition, it provides a means of maintaining a history of system documentation. The status page provides a location to archive system documentation should the need arise to review past documents. This is a useful mechanism only if certain guidelines are followed for its use.

All documents posted to the status page must have a name that easily identifies what the document is and what year/date the document was applicable. Simply adding the word “final” to a document name is insufficient as you may soon have five documents that are all labeled “final”. The status page should only be used to post completed and reviewed documents. A brief synopsis of each item on the status page is given below.

Security Authorization: This element is the repository for the concurrence, certification, and ATO memorandums.

Risk Assessment: This element should be used to maintain dates of risk assessment reviews. Risk Assessment documents are not required to be posted to the status page.

System Security Plan: This element should be used to archive the SSP. The SSP should be archived after the annual review and after receiving the concurrence memorandum.

Contingency Plan: This element should be used to maintain contingency planning status. Contingency planning documents are not required to be posted to the status page.

Contingency Plan Test: This element should be used to maintain contingency plan testing status. Contingency planning test documents are required to be posted to the status page. Therefore a history of contingency plan testing should always be available here.

E-Authentication: This element should be used to maintain E-Authentication risk assessment status. The authentication level used by the system should be entered here. The E-Authentication risk assessment documents are not required to be posted to the status page.

Configuration Management: This element should be used to maintain configuration management plan review status. Configuration management planning documents are not required to be posted to the status page.

Incident Response: This element should be used to maintain incident response plan review status. Incident response planning documents are not required to be posted to the status page.

Miscellaneous Artifacts: This element is currently not in use by USDA.

Privacy Threshold Analysis: This element should be used to maintain PTA status. PTA documents are not required to be posted to the status page.

Personally Identifiable Information: Please identify if the system contains PII information here.

Privacy Impact Assessment: This element should be used to maintain PIA status. PIA documents are not required to be posted to the status page.

System of Record Notice ID: This element should be used to maintain SORN status. SORN documents are not required to be posted to the status page.

The CSAM appendices should maintain/contain the latest version of the document that applies to the system in question. The Status Page provides a location for archiving; the Appendix page provides a location for the current documentation. Some appendices are not yet utilized. A breakdown of CSAM appendices is listed below.

Appendix	Appendix Name	Annual review	A&A Review (Three year or major change)	Agency Signature Required	Status Page Upload?	Notes
A	Acronym List	No	Yes	No	This document does not get uploaded to the Status Page.	OCIO developed USDA-wide documents. They should be tailored by the agencies as needed and posted.
B	Definitions	No	Yes	No	This document does not get uploaded to the Status Page.	OCIO developed USDA wide documents. They should be tailored by the agencies as needed and posted.
C	Applicable Laws and References	Yes	Yes	No	This document does not get uploaded to the Status Page.	OCIO developed USDA wide documents. They should be tailored by the agencies as needed and posted.
D	Requirements Traceability Matrix	Yes	Yes	No	This document does not get uploaded to the Status Page.	After annual SSP review, post the RTM to this appendix.
E	Security Test and Evaluation Plan and Procedures	Yes	Yes	No	At the completion of Concurrency Review, the test plan should be loaded to Appendix E. New plans should be placed in consecutive numbered E appendices.	A Test Plan is required for all A&A Testing.
F	Certification Results	Yes	Yes	No	At the completion of Concurrency Review, the A&A Supporting Documentation (Residual Risk Report, Security Assessment Report, SSP) should be loaded into Appendix F.	This is the Archive Appendix for A&A Supporting Documentation (Residual Risk Report, Security Assessment Report, SSP). Appendix F maintains a record of all testing accomplished on the system during the three year ATO cycle. See example F appendix listing below.
G1	Risk Analysis Methodology	No	No	No	This document does not get uploaded to the Status Page.	OCIO developed USDA wide documentation.

Appendix	Appendix Name	Annual review	A&A Review (Three year or major change)	Agency Signature Required	Status Page Upload?	Notes
G2	Risk Assessment Results	Yes	Yes	No	This document should be generated in CSAM at the completion of the annual review, at the completion of Concurrency Review, and should be loaded into Appendix G2. It is not required that this document be uploaded through the status page.	
G3	Risk Threat Pairing Report	Yes	Yes	No	This document should be generated in CSAM at the completion of the annual review, at the completion of Concurrency Review, and should be loaded into Appendix G3. It is not required that this document be uploaded through the status page.	
G4	Residual Risk Report	Yes	Yes	No	This document should be generated in CSAM at the completion of the annual review and should be loaded into Appendix G4.	
G5	eAuthentication Risk Assessment	No	Yes	Yes	Prior to Concurrency Review this document should be loaded into Appendix G5.	This applies to all systems utilized by non-Federal personnel.
H	Certifiers Recommendation	No	No	No	Post all concur memos to the status page under A&A and then to this appendix.	This appendix was not used in the past. It is now a repository for all system concur memos from one ATO to the next ATO.
I	System Security Policy	No	No	No	Currently not used by USDA	Currently not used by USDA
J1	System Rules of Behavior – Privileged User	No	Yes	No	This document does not get uploaded to the Status Page. It should be reviewed and uploaded to Appendix J1 prior to Concurrency Review.	
J2	System Rules of Behavior – General User	No	Yes	No	This document does not get uploaded to the Status Page. It should be reviewed and uploaded to Appendix J2 prior to Concurrency Review.	
K1	Security Operating Procedures	No	No	No	Currently not used by USDA	Currently not used by USDA
K2	MOU/SLA Agreements	No	No	No	Currently not used by USDA	Currently not used by USDA
L	Contingency Plan (s)	Yes	Yes	Yes	All current contingency planning documents are to be placed in consecutive numbered	All contingency planning test documents get placed on the status page, the most resent test results get

Appendix	Appendix Name	Annual review	A&A Review (Three year or major change)	Agency Signature Required	Status Page Upload?	Notes
					L appendices.	placed in consecutive numbered L appendices.
M	Security Awareness and Training Plan	No	No	No	Currently not used by USDA	Currently not used by USDA
N	Personnel Controls and Technical Security Controls	No	No	No	Currently not used by USDA	Currently not used by USDA
O	Incident Response Plan	Yes	Yes	Yes	This document should be loaded into Appendix O at the completion of the annual review, and prior to Concurrency Review	
Q	Configuration Management	No	Yes	Yes	Prior to Concurrency Review this document should be loaded into Appendix Q.	Configuration management may utilize more than one appendix. They would be numbered accordingly. Q1, Q2..
R	Accreditation Statement and Documentation	No	No	No	Post all letters to the Status page under A&A then post only the current ATO Letter to this appendix.	This appendix was not used in the past. It is now a repository for current ATO for the system. ATO letters also get posted to the Status Page.
S	Hardware Listing	Yes	Yes	No	This document does not get uploaded to the Status Page. Annually, at the completion of the annual review but prior to annual testing, and prior to RMF Step 3 Concurrency Review this document should be loaded to Appendix S.	
T	Software Listing	Yes	Yes	No	This document does not get uploaded to the Status Page. Annually, at the completion of the annual review but prior to annual testing, and prior to RMF Step 3 Concurrency Review this document should be loaded to Appendix T.	
U	OMB A-123 Appendix A Cycles	No	No	No	Currently not used by USDA	Currently not used by USDA
V1	Privacy Guidance	No	No	No	Currently not used by USDA	Currently not used by USDA
V2	Privacy Threshold Analysis	No	Yes	Yes	Prior to Concurrency Review this document should be loaded into Appendix V2.	
V3	Privacy Impact Assessment	No	Yes	Yes	Prior to Concurrency Review this document should be loaded into Appendix V3.	
V4	System of Records Notice	No	Yes	Yes	Prior to Concurrency Review this document	

Appendix	Appendix Name	Annual review	A&A Review (Three year or major change)	Agency Signature Required	Status Page Upload?	Notes
					should be loaded into Appendix V3.	
W1	Wireless Inventory	Yes	Yes	No	Prior to Concurrency Review this document should be loaded into Appendix V4.	Optional Appendix. This appendix is required if the system contains wireless components.

Appendix F is the repository of the residual annual artifacts supporting the continuous A&A process. This section contains the last three years of assessment information/artifacts ensuring that, at any time, a review can be performed ensuring that all controls were tested over a three year period. Below is an example of the use of the CSAM F appendix for a system in continuous A&A over the next three years:

F1: FY13 A&A Residual Risk Report
F2: FY13 A&A Security Assessment Report - Applicable
F3: FY13 A&A Security Assessment Report - Hybrid
F4: FY13 A&A Assessment Evidence
F5: FY13 A&A Concurrency Review Checklists
F6: FY13 A&A Security Plan
F7: FY14 A&A Residual Risk Report
F8: FY14 A&A Security Assessment Report - Applicable
F9: FY14 A&A Security Assessment Report - Hybrid
F10: FY14 A&A Assessment Evidence
F11: FY14 A&A Concurrency Review Checklists
F12: FY14 A&A Security Plan
F13: FY15 A&A Residual Risk Report
F14: FY15 A&A Security Assessment Report - Applicable
F15: FY15 A&A Security Assessment Report - Hybrid
F16: FY15 A&A Assessment Evidence
F17: FY15 A&A Concurrency Review Checklists
F18: FY15 A&A Security Plan
F19: FY16 A&A Residual Risk Report
F20: FY16 A&A Security Assessment Report - Applicable
F21: FY16 A&A Security Assessment Report - Hybrid
F22: FY16 A&A Assessment Evidence
F23: FY16 A&A Concurrency Review Checklists
F24: FY16 A&A Security Plan

3.2 Configuration Management Plan

NIST requires that every system categorized as a Moderate or a High be specifically covered by a configuration management plan (CMP). There is no requirement for every system to have its own unique CMP -- if a group of systems perform configuration management the same way, they can be grouped together under a single CMP. The current CMP template is available in Appendix B of this document. The completed CMP is posted to CSAM Appendix Q.

3.3 Contingency Plan

The contingency plan (CP) provides established procedures for the assessment and recovery of a system following a system disruption. The CP provides key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of a system. All USDA systems must be specifically covered by a contingency plan (CP). This does not mean that every system must have a unique CP; it means that systems that are configured and recovered similarly can be covered by a single CP.

NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, refers to a DRP as one that addresses facility-level information system planning and a CP applies to the recovery of a system after a disruption. Once a DRP has transferred a system to an alternate location, the CP is used to restore, recover, and test systems, and put them into operation. The current CP template is available in Appendix B of this document. All CP documents get posted to CSAM Appendix L with all test documents posted through the CSAM Status Page to CSAM Appendix L.

3.3.1 Contingency Plan Testing

Each of the three CP templates (FIPS 199 low, moderate, and high) included as appendices to this guide contain details for conducting testing, training, and exercise (TT&E) activities appropriate to their respective impact level.

- **For low-impact systems**, a tabletop exercise accomplished at least annually is sufficient. The tabletop should simulate a disruption, include all main CP points of contact, and be conducted by the System Owner or responsible authority.
- **For moderate-impact systems,** a functional exercise accomplished at least annually will be conducted. The functional exercise should include all CP points of contact and be facilitated by the System Owner or responsible authority. Exercise procedures should be developed to include an element of system recovery from backup media.
- **For high-impact systems,** a full-scale functional exercise accomplished at least annually will be conducted. The full-scale functional exercise should include a system failover to the alternate location. This could include additional activities such as full notification and response of key personnel to the recovery location, recovery of a server or database from backup media or setup, and processing from a server at an

alternate location. The test should also include a full recovery and reconstitution of the information system to a known state.

The table below presents a sample TT&E activity using NIST SP 800-53 guidance and as required by the FIPS 199 impact level *(from NIST 800-34)*

Table 3-6: CP TT&E Activities TT&E Event	Sample Activity	FIPS 199 Availability Security Objective
CP Training (CP-3)	A seminar and/or briefing used to familiarize personnel with the overall CP purpose, phases, activities, and roles and responsibilities.	Low Impact = Yes Mod. Impact = Yes High Impact = Yes
Instruction (CP-3)	Instruction of contingency personnel on their roles and responsibilities within the CP and includes refresher training. (For a high-impact system, incorporate simulated events.)	Low Impact = Yes Mod. Impact = Yes High Impact = Yes
Contingency Plan Test / Exercise (CP-4)	Test and/or exercise the contingency plan to determine effectiveness and the organization's readiness. This could include planned and unplanned maintenance activities	Low Impact = Yes Mod. Impact = Yes High Impact = Yes
Tabletop Exercise (CP-4)	Discussion-based simulation of an emergency situation in an informal, stress-free environment; designed to elicit constructive scenario-based discussions for an examination of the existing CP and individual state of preparedness.	Low Impact = Yes Mod. Impact = No High Impact = No
TT&E Event FIPS 199 Availability Sample Activity Security Objective Functional Exercise (CP-4)	Simulation of a disruption with a system recovery component such as backup tape restoration or server recovery.	Low Impact = No Mod. Impact = Yes High Impact = Yes
Full-Scale Functional Exercise (CP-4)	Simulation prompting a full recovery and reconstitution of the information system to a known state and ensures that staff are familiar with the alternate facility.	Low Impact = No Mod. Impact = No High Impact = Yes
Alternate Processing Site Recovery (CP-4,CP-7)	Test/exercise the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and evaluate the site's capabilities to support contingency operations. Includes a full recovery and return to normal operations to a known secure state. (For a high-impact system, the alternate site should be fully configured as defined in the plan.)	Low Impact = No Mod. Impact = No High Impact = Yes
System Backup (CP-9)	Test backup information to verify media reliability and information integrity. (For a high-impact system, use sample backup information and ensure that backup copies are stored in a separate facility.)	Low Impact = No Mod. Impact = Yes High Impact = Yes

3.4 Disaster Recovery Plan

In accordance with NIST SP 800-34 Rev. 1, the disaster recovery Plan (DRP) is a facility recovery plan. A DRP identifies the processes and procedures to be used for the temporary relocation of one or more systems if the primary system site becomes damaged or uninhabitable. Systems without an alternate operation location are not required to develop a DRP. A USDA DRP template is planned to be released

3.5 Interconnection Security Agreement

The ISA is a security document that specifies the technical and security requirements for establishing, operating, and maintaining an interconnection. With NIST SP 800-53 Rev. 3, the requirements have become more stringent and the concurrency review team will be specifically looking for some form of ISA for every connection where the AOs for the two connected systems are different. NIST SP 800-47 recommends an ISA as well as a memorandum of understanding (MOU) be utilized for each connection. OCD has combined the information required for both documents into a single ISA template. The current template can be found in Appendix B of this document.

All ISAs should be uploaded into CSAM through the Relationships Table. The Relationships Table can also be used to archive old versions of the ISA.

ISAs must be re-established every three years with the ATO and re-posted to the Relationships Table in CSAM. They must be reviewed annually and signed off on the "System Annual Review Memo" which can be found in Appendix B of this document.

3.6 E-Authentication Risk Assessment

OMB Memorandum 04-04 (M04-04), *E-Authentication Guidance for Federal Agencies,* requires additional attention be given to e-Government systems. An e-Government system is one that is accessible by the public. M04-04 applies to the authentication of the public user to an e-Government system. Any system accessible by the public must fill out the e-Authentication Risk Assessment and post it to CSAM Appendix G-5. A template for the e-Authentication Risk Assessment can be found in Appendix B of this document.

3.7 Incident Response Plan

NIST SP 800-53 Rev. 3 requires that each system be covered by an IRP. It is common for each agency to have an IRP that covers the entire agency. Like the CP, it is possible for a system to have its own unique IRP, or a single IRP may cover multiple systems. The IRP must be posted to CSAM Appendix O for one or more of the systems. For an IRP that covers multiple systems, the System Owner must create a document to be used by/posted for the other systems that identifies the system that contains the actual IRP. A USDA IRP template is being created and is not yet available.

3.8 Concurrency Review

The concurrency review process has been growing and adapting with the changes and requirements instituted by NIST SP 800-53 Rev 3 and NIST SP 800-37 Rev 1. Concurrency review is a USDA-instituted process used to review agency A&A documentation for compliance with NIST and Departmental guidance. Two concurrency reviews are now required for every system: the first occurs at the completion of Step 3 (formerly Phase 1) and the second at the completion of Step 4a (formerly Phase 2). The second review was implemented to minimize changes to the SSP after the assessments of Step 4 are completed. The primary purpose of the Step 3 review is to ensure that the SSP and the system categorization are correct and ready for testing/validation. If the remaining documents (IRP, CP, CMP, ISA/MOU) are provided during the Step 3 review, they will be reviewed at the time of submission. If not, they will be evaluated during the Step 4 review. The concurrency review checklists are included as Appendix C of this document.

3.9 Plan of Action and Milestones

Every SSP control that is identified as planned or not in place is required to be entered into CSAM as a POA&M. Every item from the residual risk report must be associated with an active POA&M. For a complete guide to handling POA&Ms, please refer to the POA&M guide included in Appendix D of this document.

3.10 Documenting Contractor Provided Services (Systems) in CSAM

Listed below is abbreviated guidance for entering information into CSAM for contractor provided services that would fall under the heading of software as a service (SaaS). This guidance is not applicable for most contractor systems as there are a number of systems at USDA that fall under the FISMA defined heading of Contractor Systems. This guidance is applicable to those systems that are provided as a service to USDA. USDA has nothing to do with the management and maintenance of the system and little to do with the operation of the system (limited to system user actions such as creation, modification, or deletion of users). If you have questions, please email cyber.communication@usda.gov.

1. **CSAM "System Information" "System Identification" Tab:** populate with the data available; be sure to select the contractor system checkbox. Please contact concurrency review manager at cyber.communication@usda.gov for questions concerning whether the service/system provided is a cloud system.
2. **CSAM "System Information" "Information Types" Tab:** populate with the proper security categorization information.
3. **CSAM "System Information" "Locations" Tab**: populate with the system's physical location information.
4. **CSAM "System Information" "Relationships" Tab:** populate with the applicable USDA and primary system interfaces (upload pertinent Interconnection Security Agreements (ISA).)
5. **CSAM "System Information" "Points of Contact" Tab:** populate with applicable USDA and "Provider" system points of contact.
6. **Narrative Sections 9/10:** modify these narrative sections to briefly explain what the system is and where the system security plan (SSP) can be found (e.g. in the Status and Appendix I-1 sections).
7. **Documentation uploaded into CSAM:**
   NOTE: To provide for retention of past versions of the SSP, Contingency Plans, etc., all documents below (where indicated) are uploaded first to the status page and the date updated reflecting its status, and then linked/uploaded to the appropriate appendix. When new versions of the documents are uploaded to the status page, the old one should be replaced in the appendix section. Only the current "in force" version of each document is kept/linked/uploaded to the appropriate appendix entry.

- **System SSP:** post to the CSAM "Status" Tab under "System Security Plan" and associate/link to Appendix I-1 (The SSP is a required document.)
- **Contingency Plan/Disaster Recovery Plan:** post to the CSAM "Status" Tab under "Contingency Plan" and associate/link to Appendix L (The contingency plan is a required document.)

  If there are multiple/additional contingency plan/disaster recovery planning documents, they should be posted to the CSAM "Status" Tab under "Contingency Plan" and associated/linked to Appendix Lx (where "x" is a sequential number).
- **Configuration Management Plan:** post to the CSAM "Status" Tab under "Configuration Management" and associate/link to Appendix Q (The configuration management plan is a required document for moderate and high systems.)

  Additional configuration management planning documents should be posted to the CSAM "Status" Tab under "Configuration Management" and associated/linked to Appendix Qx (where "x" is a sequential number).
- **PTA and PIA:** post to the CSAM "Status" Tab under "Privacy Threshold Analysis" and "Privacy Impact Assessment" and associate/link to Appendices V2 and V3 (The PTA is a required document; the PIA is required if directed by the PTA.)
- **Hardware and software inventories:** post to Appendices S and T if these are separate documents from the SSP.
- **Rules of Behavior:** (administrative and general user as available) post to Appendices J1 and J2.
- **Memorandum of Understanding (MOU)/Service Level Agreement (SLA)/Memorandum of Agreement (MOA)/contract/agreement:** Selected contract/agreement with the providing company should be posted to Appendix K2.
- **Security Assessment Plan:** post to the CSAM Appendix E if a separate document exists.
- **Security Assessment Report:** post to the CSAM Appendix E1 (The security assessment report is a required document.)
- **Risk Assessment Report:** post to the CSAM "Status" Tab under "Risk Assessment" and associate/link to Appendix G2. If the Risk Assessment and the Security Assessment Report are combined as a single document, post the document under both Appendix E1 and G2. (The Risk Assessment is a required document.)
- **POA&M report:** post to Appendix G4 (The system POA&M is a required document.)

- **E-Authentication Risk Assessment:** (also known as OMB Memorandum 04-04): post to the CSAM "Status" Tab under "E-Authentication" and associate/link to Appendix G5.
- **Assessment Evidence:** post to Appendix G6 if not part of the Security Assessment Report.
- **Incident Response Plan:** post to the CSAM "Status" Tab under "Incident Response" and associate/link to Appendix O.
- **Security Awareness:** training plan should be posted to Appendix M.
- **Concur Memos and Authority To Operate (ATO) Letters:** post to the CSAM "Status" Tab under "Security Authorization" and then associate/link to Appendix R (concur memos and ATO letters are required documents.)

At the completion of the RMF Step 4 concurrency review the following completed documents will be posted to CSAM Appendix F by concurrency review. Appendix F is the CSAM repository for the following documents: SSP, Assessment Report, Risk Assessment, POA&Ms. These documents will be posted at the completion of every RMF Step 4 concurrency review from one ATO cycle to the next. In other words, at the completion of the annual review and assessment the system must complete concurrency review and these four documents will be posted to appendix F and will remain there until the next ATO is issued and then the oldest set of documents can be overwritten in CSAM.

4 Contact Information

OCIO established a Center of Excellence (COE) to be a focal point for the dissemination of information related to the A&A process, CSAM use, and POA&M management. The COE has established multiple communication channels to ensure that the agencies have access to the information and guidance necessary to successfully complete A&As and create the required POA&Ms. These communication channels include:

E-Mail:
For general questions and guidance for A&A related issues, contact cyber.communication@usda.gov. For submission of ATOs and any other CSAM functionality questions, contact cyber.csam@ocio.usda.gov

Training Materials, Policies and Procedures
CSAM and A&A training materials, policies and procedures can be found on the USDA Directives web page (http://www.ocio.usda.gov/directives/#3500link) and on CSAM (https://csam.usda.gov).

Concurrency Review

The concurrency review team can be reached via email at cyber.communication@usda.gov. Inserting "concurrency review" in the subject line will expedite contact by the concurrency team.

Appendix A - Acronyms

Acronym	Description
ATO	Authority to Operate
AO	Authorizing Official
A&A	Assessment and Authorization
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CMP	Configuration Management Plan
CP	Contingency Plan
CPO	Cyber Policy and Oversight
CSAM	Cyber Security Assessment Management System
DAA	Designated Approving Authority
DRP	Disaster Recovery Plan
E-AUTH	E-Authentication
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FY	Fiscal Year
IRP	Incident Response Plan
ISA	Interconnection Security Agreement
ISSPM	Information Systems Security Program Manager
IT	Information Technology
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OCD	Oversight Compliance Division
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
POA&M	Plan of Action and Milestones
PTA	Privacy Threshold Analysis
RA	Risk Assessment
Rev	Revision
SOP	Standard Operating Procedure
SORN	System of Records Notice
SP	Special Publication
SSP	System Security Plan
ST&E	Security Test and Evaluation
USDA	United States Department of Agriculture

Appendix B - A&A Templates

The A&A templates can be found on the following USDA intranet web page: http://www.ocionet.usda.gov/wps/portal/ocio/ocioportal/home/security/security_ca

Appendix C – Concurrency Review Checklists

The concurrency review checklists can be found on the following intranet Web page: http://www.ocionet.usda.gov/wps/portal/ocio/ocioportal/home/security/security_ca

Appendix D – Guides

Additional Users Guides can be found at:
http://www.ocionet.usda.gov/wps/portal/ocio/ocioportal/home/security/security_ca

Appendix E – IT Security Controls for Assessment

The Departments List of security controls was determined by a Department wide working group that defined the both the Key and a set of controls for assessment each fiscal year. The spreadsheet containing these controls is Appendix E to this guide as distributed by departmental memo annually and on the OCIO web site at: http://www.ocionet.usda.gov/wps/portal/ocio/ocioportal/home/security/security_ca

Continuous Assessment and Authorization
Control Selection Worksheet (Final)

12-10-12

NIST Base Information			Annual Security Assessment Controls Sets 1,2,3 and Key Controls			
(NIST 800-53 Rev3) with Rev 4 (Draft) Notations			Dept Annual Control Set(s)			
Control	**Enhancement**	**Applicable FIPS 199 Baseline**	**Key Controls**	**Set 1 (FY13)**	**Set 2 (FY14)**	**Set 3 (FY15) NOTE: Rev 4 Notes are Draft until NIST finalizes**
AC-1		L,M,H			Include	
AC-2		L,M,H	**Key**			
	AC-2(1)	M,H		Include		
	AC-2(2)	M,H		Include		
	AC-2(3)	M,H	**Key**			
	AC-2(4)	M,H	**Key**			
	AC-2(5)	**H**				**Rev 4 (include)**
	AC-2(12)	**H**				**Rev 4 (include)**
	AC-2(13)	**H**				**Rev 4 (include)**
AC-3		L,M,H	**Key**			
AC-4		M,H				Include
AC-5		M,H	**Key**			
AC-6		M,H	**Key**			
	AC-6(1)	M,H			include	
	AC-6(2)	M,H	**Key**			
	AC-6(3)	**H**				**Rev 4 (include)**
	AC-6(5)	**M,H**				**Rev 4 (include)**
AC-7		L,M,H			Include	
AC-8		L,M,H			Include	
AC-9		NS				
AC-10		H			Include	
AC-11		M,H			Include	
AC-12	Withdrawn - Rev 3					
AC-13	Withdrawn - Rev 3					
AC-14		L,M,H		include		
	AC-14(1)	M,H		include		**Withdrawn - Rev 4**
AC-15	Withdrawn - Rev 3					
AC-16		NS				
AC-17		L,M,H			Include	
	AC-17(1)	M,H			Include	
	AC-17(2)	M,H			Include	
	AC-17(3)	M,H			Include	
	AC-17(4)	M,H			Include	
	AC-17(5)	M,H			Include	**Withdrawn - Rev 4**
	AC-17(7)	M,H			Include	**Withdrawn - Rev 4**
	AC-17(8)	M,H			Include	**Withdrawn - Rev 4**
AC-18		L,M,H				Include
	AC-18(1)	M,H				Include
	AC-18(2)	H		Include		**Withdrawn - Rev 4**
	AC-18(4)	H			Include	
	AC-18(5)	H				Include
AC-19		L,M,H		Include		
	AC-19(1)	**M,H**		Include		**Withdrawn - Rev 4**
	AC-19(2)	**M,H**		Include		**Withdrawn - Rev 4**
	AC-19(3)	**M,H**		Include		**Withdrawn - Rev 4**

(NIST 800-53 Rev3) with Rev 4 (Draft) Notations			Dept Annual Control Set(s)			
Control	Enhancement	Applicable FIPS 199 Baseline	Key Controls	Set 1 (FY13)	Set 2 (FY14)	Set 3 (FY15) NOTE: Rev 4 Notes are Draft until NIST finalizes
Errata	AC-19(6)	M,H		~~Include~~		Rev 4 (include)
AC-20		L,M,H				include
	AC-20(1)	M,H				Include
	AC-20(2)	M,H				Include
AC-21		NS				
AC-22		L,M,H			Include	
AC-23		NS				Rev 4 - Not Selected
AC-24		NS				Rev 4 - Not Selected
AC-25		NS				Rev 4 - Not Selected
AT-1		L,M,H			Include	
AT-2		L,M,H		Include		
	AT-2(2)	M,H				Rev 4 (include)
AT-3		L,M,H		include		
AT-4		L,M,H		include		
AT-5		NS				
AT-5		M,H				Rev 4 (include)
AU-1		L,M,H		Include		
AU-2		L,M,H	Key			
	AU-2(2)	M,H			Include	
	AU-2(3)	M,H			Include	
	AU-2(4)				include	
AU-3		L,M,H	Key			
	AU-3(1)	M,H			Include	
	AU-3(2)	H			Include	
AU-4		L,M,H		Include		
AU-5		L,M,H	Key			
	AU-5(1)	H		Include		
	AU-5(2)	H		Include		
AU-6		M,H	Key			
	AU-6(1)	M,H				Modified - Rev4 (Include)
	AU-6(3)	M,H				Rev 4 (include)
	AU-6(5)	H				Rev 4 (include)
	AU-6(6)	H				Rev 4 (include)
	AU-6(9)	M,H				Rev 4 (include)
AU-7		M,H				include
	AU-7(1)	M,H				include
AU-8		L,M,H			Include	
	AU-8(1)	M,H			Include	
AU-9		L,M,H				Include
	AU-9(2)	H				Rev 4 (include)
	AU-9(3)	H				Rev 4 (include)
	AU-9(4)	M,H				Rev 4 (include)
AU-10		NS				
AU-11		L,M,H			include	
AU-12		L,M,H	Key			
	AU-12(1)	H				Include
	AU-12(3)	H				Rev 4 (include)

Continuous Assessment and Authorization
Control Selection Worksheet (Final)

(NIST 800-53 Rev3) with Rev 4 (Draft) Notations			Dept Annual Control Set(s)			
Control	Enhancement	Applicable FIPS 199 Baseline	Key Controls	Set 1 (FY13)	Set 2 (FY14)	Set 3 (FY15) NOTE: Rev 4 Notes are Draft until NIST finalizes
AU-13		NS				
AU-14		NS				
AU-15						Rev 4 (include)
AU-16						Rev 4 (include)
CA-1		L,M,H		Include		
CA-2		L,M,H		Include		
	CA-2(1)			Include		
	CA-2(2)			Include		
CA-3		L,M,H	Key			
CA-4	Withdrawn - Rev 3					
CA-5		L,M,H			Include	
CA-6		L,M,H			Include	
CA-7		L,M,H				Include
	CA-7(1)	M,H				Rev 4 (include)
CM-1		L,M,H			Include	
CM-2		L,M,H	Key			
	CM-2(1)	M,H	Key			
	CM-2(2)	H		include		
	CM-2(3)	M,H		include		
	CM-2(4)	M,H		include		Withdrawn - Rev 4
	CM-2(5)	H		include		Withdrawn - Rev 4
	CM-2(6)	H		include		
CM-3		M,H	Key			
	CM-3(1)	H			include	
	CM-3(2)	M,H			Include	
CM-4		M,H				Include
	CM-4(1)					Include
CM-5		M,H	Key			
	CM-5(1)	H		Include		
	CM-5(2)	H		Include		
	CM-5(3)	H		Include		
CM-6		L,M,H	Key			
	CM-6(1)	H			Include	
	CM-6(2)	H			Include	
	CM-6(3)	M,H			Include	Withdrawn - Rev 4
CM-7		M,H	Key			
	CM-7(1)	M,H				Include
	CM-7(2)	H				Include
	CM-7(4)	M				Rev 4 (include)
	CM-7(5)	H				Rev 4 (include)
CM-8		L,M,H			Include	
	CM-8(1)	M,H			Include	
	CM-8(2)	H			Include	
	CM-8(3)	H			Include	
	CM-8(4)	H			Include	
	CM-8(5)	M,H			Include	
	CM-8(6)	H			Include	

Continuous Assessment and Authorization
Control Selection Worksheet (Final)

(NIST 800-53 Rev3) with Rev 4 (Draft) Notations			Dept Annual Control Set(s)			
Control	Enhancement	Applicable FIPS 199 Baseline	Key Controls	Set 1 (FY13)	Set 2 (FY14)	Set 3 (FY15) NOTE: Rev 4 Notes are Draft until NIST finalizes
CM-9		M,H			Include	
CM-10		L,M,H				Rev 4 (include)
CM-11		L,M,H				Rev 4 (include)
CP-1		L,M,H			Include	
CP-2		L,M,H				Include
	CP-2(1)	M,H				Include
	CP-2(2)	H				Include
	CP-2(3)	M,H				Modified - Rev 4 (include)
	CP-2(4)	H				Rev 4 (include)
	CP-2(5)	H				Rev 4 (include)
	CP-2(8)	M,H				Rev 4 (include)
CP-3		L,M,H		Include		
	CP-3(1)	H		Include		
CP-4		L,M,H	Key			
	CP-4(1)	M,H		Include		
	CP-4(2)	H		Include		
	CP-4(4)	H		Include		
CP-5						Rev 4 (include)
CP-6		M,H		Include		
	CP-6(1)	M,H		Include		
	CP-6(2)	H		Include		
	CP-6(3)	M,H		Include		
CP-7		L,M,H			Include	
	CP-7(1)	M,H			Include	
	CP-7(2)	M,H			Include	
	CP-7(3)	M,H			Include	
	CP-7(4)	H			Include	
	CP-7(5)	M,H			Include	Withdrawn - Rev 4
CP-8		M,H			Include	
	CP-8(1)	M,H			Include	
	CP-8(2)	M,H			Include	
	CP-8(3)	H			Include	
	CP-8(4)	H			Include	
CP-9		L,M,H	Key			
	CP-9(1)	M,H				include
	CP-9(2)	H				include
	CP-9(3)	H				include
	CP-9(5)	H				Rev 4 (include)
CP-10		L,M,H				include
	CP-10(2)	M,H				include
	CP-10(3)	M,H				include
	CP-10(4)	H				include
	CP-10(5)	H				Rev 4 (include)
CP-11		H				Rev 4 (include)
CP-12		NS				Rev 4 - Not Selected
CP-13		NS				Rev 4 - Not Selected

(NIST 800-53 Rev3) with Rev 4 (Draft) Notations			Dept Annual Control Set(s)			
Control	Enhancement	Applicable FIPS 199 Baseline	Key Controls	Set 1 (FY13)	Set 2 (FY14)	Set 3 (FY15) NOTE: Rev 4 Notes are Draft until NIST finalizes
IA-1		L,M,H			include	
IA-2		L,M,H		Include		
	IA-2(1)	L,M,H		Include		
	IA-2(2)	M,H		Include		
	IA-2(3)	M,H		Include		
	IA-2(4)	H		Include		
	IA-2(8)	M,H		Include		
	IA-2(9\)	H		Include		
IA-3		M,H			Include	
IA-4		L,M,H	Key			
IA-5		L,M,H			include	
	IA-5(1)	L,M,H	Key			
	IA-5(2)	M,H			include	
	IA-5(3)	M,H			include	
IA-6		L,M,H			include	
IA-7		L,M,H			Include	
IA-8		L,M,H		include		
IA-9		NS				Rev 4 - Not Selected
IA-10		NS				Rev 4 - Not Selected
IA-11		NS				Rev 4 - Not Selected
IA-12		NS				Rev 4 - Not Selected
IR-1		L,M,H			Include	
IR-2		L,M,H		Include		
	IR-2(1)	H		Include		
	IR-2(2)	H		Include		
IR-3		L,M,H				include
	IR-3(1)	H				include
	IR-3(2)	M,H				Rev 4 (include)
IR-4		M,H				include
	IR-4(1)	M,H				include
	IR-4(4)	H				Rev 4 (include)
IR-5		L,M,H				include
	IR-5(1)	H				include
IR-6		L,M,H				include
	IR-6(1)	M,H				include
IR-7		L,M,H			include	
	IR-7(1)	M,H			Include	
IR-8		L,M,H			include	
IR-9		NS				Rev 4 - Not Selected
MA-1		L,M,H				include
MA-2		L,M,H		Include		
	MA-2(1)	M,H		Include		
	MA-2(2)	H		Include		Withdrawn - Rev 4
MA-3		M,H			Include	
	MA-3(1)	M,H			Include	
	MA-3(2)	M,H			Include	
	MA-3(3)	H			Include	

Continuous Assessment and Authorization
Control Selection Worksheet (Final)

(NIST 800-53 Rev3) with Rev 4 (Draft) Notations			Dept Annual Control Set(s)			
Control	Enhancement	Applicable FIPS 199 Baseline	Key Controls	Set 1 (FY13)	Set 2 (FY14)	Set 3 (FY15) NOTE: Rev 4 Notes are Draft until NIST finalizes
MA-4		L,M,H		Include		
	MA-4(1)	M,H		Include		
	MA-4(2)	M,H		Include		
	MA-4(3)	H		Include		
MA-5		L,M,H				Include
	MA-5(1)	H				Rev 4 (include)
MA-6		M,H			Include	
MP-1		L,M,H				Include
MP-2		L,M,H			Include	
	MP-2(1)	M,H			Include	
MP-3		M,H		Include		
MP-4		M,H		Include		
MP-5		M,H		include		
	MP-5(2)	M,H		Include		Withdrawn - Rev 4
	MP-5(3)	H		Include		
	MP-5(4)	M,H		Include		
MP-6		L,M,H			Include	
	MP-6(1)	H			Include	
	MP-6(2)	H			Include	
	MP-6(3)	H			include	
MP-7		L,M,H				Rev 4 (include)
	MP-7(1)	M,H				Rev 4 (include)
	MP-7(2)	M,H				Rev 4 (include)
MP-8		NS				Rev 4 - Not Selected
PE-1		L,M,H				include
PE-2		L,M,H			Include	
PE-3		L,M,H			include	
	PE-3(1)	H			include	
PE-4		H			include	
PE-5		M,H		Include		
PE-6		L,M,H		Include		
	PE-6(1)	M,H		Include		
	PE-6(2)	H		Include		
PE-7		L,M,H		Include		Withdrawn - Rev 4
	PE-7(1)	M,H		Include		Withdrawn - Rev 4
PE-8		L,M,H		Include		
	PE-8(1)	H		Include		
	PE-8(2)	H		Include		Withdrawn - Rev 4
PE-9		M,H			Include	
PE-10		M,H			include	
PE-11		M,H			include	
	PE-11(1)	H			include	
PE-12		L,M,H			Include	
PE-13		L,M,H		Include		
	PE-13(1)	M,H		Include		
	PE-13(2)	M,H		Include		
	PE-13(3)	M,H		Include		

(NIST 800-53 Rev3) with Rev 4 (Draft) Notations			Dept Annual Control Set(s)			
Control	Enhancement	Applicable FIPS 199 Baseline	Key Controls	Set 1 (FY13)	Set 2 (FY14)	Set 3 (FY15) NOTE: Rev 4 Notes are Draft until NIST finalizes
PE-14		L,M,H			Include	
PE-15		L,M,H			Include	
	PE-15(1)	H			Include	
PE-16		L,M,H		Include		
PE-17		M,H		Include		
PE-18		M,H		Include		
	PE-18(1)	M,H		Include		Withdrawn - Rev 4
PE-19		NS				
PE-20		NS				Rev 4 - Not Selected
PL-1		L,M,H				include
PL-2		L,M,H			include	
PL-3	Withdrawn - Rev 3					
PL-4		L,M,H			include	
PL-5		L,M,H		Include		Withdrawn - Rev 4
PL-6		L,M,H		Include		Withdrawn - Rev 4
PL-7		NS				Modified - Rev 4 - NS
PL-8		NS				Rev 4 - Not Selected
PM-01		L,M,H				include
PM-02		L,M,H				include
PM-03		L,M,H			include	
PM-04		L,M,H			Include	
PM-05		L,M,H			Include	
PM-06		L,M,H		Include		
PM-07		L,M,H		Include		
PM-08		L,M,H				include
PM-09		L,M,H			include	
PM-10		L,M,H			include	
PM-11		L,M,H			include	
PM-12		L,M,H				Rev 4 (include)
PM-13		L,M,H				Rev 4 (include)
PM-14		L,M,H				Rev 4 (include)
PM-15		L,M,H				Rev 4 (include)
PS-1		L,M,H		Include		
PS-2		L,M,H		Include		
PS-3		L,M,H		Include		
PS-4		L,M,H	Key			
	PS-4(1)	H				Rev 4 (include)
	PS-4(2)	H				Rev 4 (include)
PS-5		L,M,H			Include	
PS-6		L,M,H			Include	
PS-7		L,M,H				include
	PS-7(1)	M,H				Rev 4 (include)
PS-8		L,M,H				include
	PS-8(1)	M,H				Rev 4 (include)
RA-1		L,M,H				include
RA-2		L,M,H		Include		
RA-3		L,M,H		Include		

Continuous Assessment and Authorization
Control Selection Worksheet (Final)

(NIST 800-53 Rev3) with Rev 4 (Draft) Notations			Dept Annual Control Set(s)			
Control	Enhancement	Applicable FIPS 199 Baseline	Key Controls	Set 1 (FY13)	Set 2 (FY14)	Set 3 (FY15) NOTE: Rev 4 Notes are Draft until NIST finalizes
RA-4	Withdrawn - Rev 3					
RA-5		L,M,H	Key			
	RA-5(1)	M,H			Include	
	RA-5(2)	H			Include	
	RA-5(3)	H			Include	
	RA-5(4)	H			Include	
	RA-5(5)	H			Include	
	RA-5(6)	H			Include	
	RA-5(7)	H			Include	
	RA-5(8)	H			Include	
	RA-5(9)	H			Include	
SA-1		L,M,H				include
SA-2		L,M,H			Include	
SA-3		L,M,H		Include		
SA-4		L,M,H		Include		
	SA-4(1)	M,H		Include		
	SA-4(2)	H		Include		
	SA-4(4)	M,H		Include		
SA-5		L,M,H				include
	SA-5(1)	M,H				include
	SA-5(2)	H				include
	SA-5(3)	M,H				include
	SA-5(6)	M,H				Rev 4 (include)
SA-6		L,M,H		Include		Withdrawn - Rev 4
SA-7		L,M,H		Include		Withdrawn - Rev 4
SA-8		M,H		Include		
SA-9		L,M,H				include
	SA-9(2)	M,H				Rev 4 (include)
	SA-9(3)	H				Rev 4 (include)
SA-10		M,H			Include	
SA-11		M,H			Include	
SA-12		H			Include	
SA-13		H			Include	Withdrawn - Rev 4
SA-14		NS				
SA-15		H				Rev 4 (include)
SA-16		H				Rev 4 (include)
SA-17		H				Rev 4 (include)
SA-18		NS				Rev 4 - Not Selected
SA-19		NS				Rev 4 - Not Selected
SC-1		L,M,H				include
SC-2		M,H				include
SC-3		H				include
	SC-3(6)	H				Rev 4 (include)
SC-4		M,H		Include		
SC-5		L,M,H		Include		
SC-6		NS				
SC-7		L,M,H	Key			

(NIST 800-53 Rev3) with Rev 4 (Draft) Notations			Dept Annual Control Set(s)			
Control	Enhancement	Applicable FIPS 199 Baseline	Key Controls	Set 1 (FY13)	Set 2 (FY14)	Set 3 (FY15) NOTE: Rev 4 Notes are Draft until NIST finalizes
	SC-7(1)	M,H		Include		
	SC-7(2)	M,H		Include		Withdrawn - Rev 4
	SC-7(3)	M,H		Include		
	SC-7(4)	M,H		Include		
	SC-7(5)	M,H		Include		
	SC-7(6)	H		Include		
	SC-7(7)	M,H		Include		
	SC-7(8)	H		Include		
SC-8		M,H			include	
	SC-8(1)	M,H			include	
SC-9		M,H	Key			
	SC-9(1)	M,H			Include	
SC-10		M,H			Include	
					Include	
SC-11		NS				
SC-12		L,M,H				include
	AC-12(1)	H				include
SC-13		L,M,H				include
SC-14		L,M,H				include
SC-15		L,M,H			include	
SC-16		NS				
SC-17		M,H			include	
SC-18		M,H			include	
SC-19		M,H			include	
SC-20		L,M,H				include
	SC-20(1)	L,M,H		Include		Withdrawn - Rev 4
SC-21		L,M,H				Modified - Rev 4 (include)
SC-22		L,M,H				Modified - Rev 4 (include)
SC-23		M,H		include		Withdrawn - Rev 4
SC-24		H				include
SC-25		NS				
SC-26		NS				
SC-27		NS				
SC-28		M,H		Include		
SC-29		NS				
SC-30		NS				
SC-31		NS				
SC-32		M,H		include		
SC-33		NS				
SC-34		NS				
SC-35		NS				Rev 4 - Not Selected
SC-36		NS				Rev 4 - Not Selected
SC-37		NS				Rev 4 - Not Selected
SC-38		NS				Rev 4 - Not Selected
SC-39		NS				Rev 4 - Not Selected
SC-40		NS				Rev 4 - Not Selected
SC-41		L,M,H				Rev 4 (include)

Continuous Assessment and Authorization
Control Selection Worksheet (Final)

12-10-12

(NIST 800-53 Rev3) with Rev 4 (Draft) Notations			Dept Annual Control Set(s)			
Control	Enhancement	Applicable FIPS 199 Baseline	Key Controls	Set 1 (FY13)	Set 2 (FY14)	Set 3 (FY15) NOTE: Rev 4 Notes are Draft until NIST finalizes
SC-42		NS				Rev 4 - Not Selected
SI-1		L,M,H				include
SI-2		L,M,H		Include		
	SI-2(1)	H		Include		
	SI-2(2)	M,H		Include		
SI-3		L,M,H		Include		
	SI-3(1)	M,H		Include		
	SI-3(2)	M,H		Include		
	SI-3(3)	M,H		Include		
SI-4		L,M,H				Modified - Rev 4 (Include)
	SI-4(2)	M,H				include
	SI-4(4)	M,H				include
	SI-4(5)	M,H				include
	SI-4(6)	M,H				include
SI-5		L,M,H		Include		
	SI-5(1)	H		include		
SI-6		H		Include		
SI-7		H				include
	SI-7(1)	H				include
	SI-7(2)	H				include
	SI-7(5)	H				Rev 4 (include)
	SI-7(8)	M,H				Rev 4 (include)
	SI-7(15)	H				Rev 4 (include)
SI-8		M,H				include
	SI-8(1)	M,H				include
	SI-8(2)	M,H				Rev 4 (include)
SI-9		M,H			Include	
SI-10		M,H	Key			
SI-11		M,H			Include	
SI-12		M,H			Include	
SI-13		NS				Withdrawn - Rev 4
SI-14		NS				Rev 4 - Not Selected
245	213		28	120	123	70

Cat	Key Controls (Test Annually)	Set 1 (Test in FY13)	Set 2 (Test in FY14)	Set 3 (Text in FY 15)
Low	16	39	40	29
Mod	28	89	90	53
High	28	118	121	69

USDA NATIONAL INFORMATION TECHNOLOGY CENTER (NITC)

Appendix A –Midrange

Midrange Hosting Services

FY2014

Midrange PaaS

Midrange IaaS

Managed Hosting

Collocation Hosting

Washington DC Computing Facility

Midrange Hosting Services includes varying levels of hosting services that include NITC owned and managed Infrastructure as a Service as well as traditional NITC-managed and customer-managed hosting of customer-owned equipment.

Appendix A –Midrange

Table of Contents

1 Hosting Types and Platforms 5

1.1 Hosting Types 5

1.1.1 PaaS Server Hosting Services 7

1.1.2 IaaS - Server Hosting Services 10

1.1.3 Midrange Managed Hosting Services 10

1.1.4 Midrange Collocation Services 11

1.1.5 Washington DC Computing Facility Services 11

1.2 Platforms 14

1.2.1 Windows Platform 14

1.2.2 Linux Platform 14

1.2.3 AIX Platform 15

1.2.4 Solaris Platform 15

2 Security 15

2.1 Midrange System Security Services 16

2.1.1 Central Authentication Solutions 16

2.1.2 Identity Manager 16

2.1.3 Elevated Privilege Access Control 16

2.1.4 Security Baseline Configuration 17

2.1.5 Digital Certificates and Multi-Factor Authentication 17

2.1.6 Enterprise Risks 17

2.2 Security Assessment Services (Scanning) 17

2.3 Certification and Accreditation (C&A) 18

2.3.1 Inheritance of Controls 19

2.3.2 Interconnection Security Agreements (ISA) 19

3 System Administration 19

3.1 Standard Service Activities 19

3.2 System deployment 20

3.3 Baseline Configuration Standards 20

3.4 Operating System Upgrades & Patches 22

3.5 System Backups 24

3.5.1 Midrange Managed Hosting Backup Strategies 24

3.5.2 PaaS Midrange (AIX) Backup Strategies 24

3.5.3 PaaS Midrange (Solaris) Backup Strategies........24
3.5.4 PaaS Midrange (x86) Backup Strategies........24
3.6 Audit Logging........24
4 Contract Management........25
4.1 Billing........25
4.2 Procurement........25
5 Disaster Recovery........26
5.1 The Heart of Disaster Recovery at the NITC........26
5.1.1 HA Core Network........26
5.1.2 Access Layer........27
5.1.3 Storage Services Layer........27
5.2 How the NITC DR Solution Works........27
5.2.1 Technical Summary........27
5.2.2 Five General Steps to a Disaster Recovery Exercise at the NITC........28
5.2.3 Seven Steps to a True Disaster Recovery........28
5.2.4 Other Technical Considerations........28
5.3 Disaster Recovery Testing........28
5.4 Declaring a Disaster........29
5.5 Available Disaster Recovery Methods........29
5.5.1 SAN Mirroring........30
5.5.2 VMware’s Site Recovery Manager........30
5.5.3 Disk Based Backup Strategy........30
5.5.4 Tape Shipping (Virtual and Physical)........30
5.5.5 Recommended Disaster Recovery Methods by Service Offering........30
5.6 Professional Services........31
5.7 Disaster Recovery Costs........31
5.8 Disaster Recovery Roles and Responsibilities........32
6 Midrange Services Roles and Responsibilities........32

Table of Tables

Table 1: Midrange Services Matrix........5

Appendix A –Midrange

Table 2: Supported Operating Systems for Midrange PaaS Server Hosting Services 8
Table 3: Midrange PaaS-Server Resource Configuration Guide 9
Table 4: Supported Operating Systems for Midrange Managed Hosting Services 10
Table 5: Supported Operating System Versions (Windows) 14
Table 6: Supported Operating System Versions (Linux) 14
Table 7: Supported Operating System Versions (AIX) 15
Table 8: Supported Operating System Versions (Solaris) 15
Table 9: Baseline Configuration Items 21
Table 10: Official Patching Schedule for all UNIX/LINUX and Windows-Based environments 22
Table 11: DR Roles and Responsibilities 32

Appendix A –Midrange

Midrange Hosting Services

1 Hosting Types and Platforms

1.1 Hosting Types

NITC offers four midrange hosting solutions of various types. This includes physical hosting and cloud hosting (virtualized). This section outlines the services as well as the differences between each service. For a quick reference of hosting type activities, see Table 1.

Table 1: Midrange Services Matrix

Activity		NITC Service Offering			
		Cloud Hosting		Physical Hosting	
		PaaS - Server	IaaS - Server	Midrange Managed Hosting	Collocation*
Operating Systems Support	Audit Assistance (C&A and ST&E)	$	$	$	
	Capacity Planning	✓	✓	✓	
	Custom Script Design	$	$	$	
	Decommissioning Services	$	$	$	$
	Disaster Recovery	$	$	$	$
	File System Maintenance	✓	$	✓	
	Hardware Maintenance	✓	✓	$	
	Hardware Refresh	✓	✓		
	Mail Server - Inbound	$	$	$	
	Mail Relay Services	✓	$	✓	✓
	Migration from NITC	$	$	$	$
	OS Analysis and Performance Tuning	✓	$	✓	
	OS Baseline Configuration / Hardening	✓	$	✓	
	OS Certification and Accreditation	✓	$	$	
	OS Compliance Monitoring	✓	$	✓	
	OS Patching	✓	$	✓	
	OS Software Maintenance	✓	$	✓	
	OS Troubleshooting	✓	$	✓	
	Provisioning	✓	✓	✓	
	Remote Access Management (rdp/ssh)	✓	$	✓	
	Storage Design/Integration (NITC)	✓	$	✓	$
	Storage Design/Integration (Non-NITC Storage)	$	$	$	

Appendix A –Midrange

Activity		NITC Service Offering			
		Cloud Hosting		Physical Hosting	
		PaaS - Server	IaaS - Server	Midrange Managed Hosting	Collocation*
	System Architecture/Design/Documentation	$	$	$	
	System Automation (BigFix)	✓	$	✓	✓
	System Automation (BladeLogic)	✓	$	✓	
	Virus Detection	✓	$	✓	$
	Virus Remediation	✓	$	✓	
	Vulnerability Management/Remediation	✓	$	✓	
Application Support	Application Patching	$	$	$	
	Application Administration	$	$	$	
	Application Load Testing	$	$	$	
	Application Software Installs	$	$	$	
	Application Troubleshooting	$	$	$	
	Application Vulnerability Remediation	$	$	$	
Storage	Backup and Recovery	✓	✓	✓	$
	Disaster Recovery	✓	$	✓	$
	Storage Services and Infrastructure	✓	$	✓	$
Network/Security	Central Authentication/ Active Directory / ID mgmt	✓	$	✓	✓
	Role Based Access Controls	✓	$		
	Central Logging (SIEMS)	✓	$		
	Computer Security Incident Response	✓	$	✓	✓
	Digital Certificate Management	$	$	$	$
	Domain Name Services (DNS)	✓	$	✓	✓
	Firewall Infrastructure (highly available)	✓	$	✓	✓
	Network Infrastructure (highly available)	✓	$	✓	✓
	Network Intrusion Detection	✓	$	✓	✓
	Network Remote Access	✓	$	✓	✓
	Time Synchronization Services	✓	$	✓	✓
	Troubleshooting (firewall/network)	✓	$	✓	
	Vulnerability Scanning and Reporting	✓	$	✓	
	Wireless Intrusion Detection	✓	$	✓	

Appendix A –Midrange

	Activity	NITC Service Offering			
		Cloud Hosting		Physical Hosting	
		PaaS - Server	IaaS - Server	Midrange Managed Hosting	Collocation*
	OS Account Administration (local accounts)	✓	$	✓	
	OS Administration	✓	$	✓	
ITIL	Asset Management	✓	✓	✓	
	Change Management	✓	✓	✓	
	Event/System Monitoring	✓	✓	✓	
	Help Desk	✓	✓	✓	
	Incident Response	✓	$	✓	
	License Management (outside OS)	✓	$	✓	
	Specialized System Monitoring (custom views)	✓	$	✓	
Business	Dedicated Account Manager	✓	✓	✓	✓
	Facilities and Environmental systems	✓	✓	✓	
	Procurement Services	$	$	$	
	Staffing	$	$	$	
	Equipment Transfer	$	$	$	

Legend: ✓ Activity is included in the service offering $ Activity is available in the service offering

* All collocation services within the above matrix are assumed to reside on NITC's network, NOT a customer-extended network within NITC facilities. (1.1.4.2)

1.1.1 PaaS Server Hosting Services

The NITC PaaS-Server Hosting Service offering includes robust hardware platforms that are virtualized for optimal cost efficiency and flexibility. The underlying hardware is coupled with NITC Network Services and NITC Storage Services to provide a fully managed operating platform up to and including one of the supported Operating Systems. By enforcing strict standards that streamline management efforts, the NITC PaaS-Server Hosting offering provides the most cost-effective server hosting option. However, not all business applications are an appropriate fit for a virtualized environment so while this service offering should certainly be explored first, it is possible that a given application may not fit within the service's defined parameters.

Appendix A –Midrange

Customers opting to participate PaaS- Server services receive the benefits of full server administration, hardware refresh, certification, and accreditation (up to and including the Operating System), security controls, as well as many other benefits outlined in the Midrange Services Matrix.

The NITC will provide all Operating Systems installation, support, and maintenance per NITC standards. Periodic hardware technology refresh is also included. Even though NITC must maintain control of elevated privileges in regards to the Operating System to protect the overall shared environment, customers maintain management control over their deployed applications.

Table 2: Supported Operating Systems for Midrange PaaS Server Hosting Services

	Platform		
Operating System	**X86**	**Sparc™**	**pSeries™**
Windows™	✓		
Red Hat Linux™	✓		
Solaris™		✓	
AIX™			✓

Under the PaaS-Server hosting model, NITC will provision server resources based on resource requirements and will actively manage resources to ensure proper performance. Since PaaS- Server hosting costs are recovered through billing based on actual configurations, hosting cost are kept to a minimum and only increase as application hosting requirements increase. This right sizing approach leads to streamlined systems and lower costs for the NITC's customers.

All Midrange PaaS-Server hosting services are provisioned and maintained within the NITC Configuration Management process to ensure supportability and reliability for the supported operating systems. The framework used by NITC is aligned with other industry Enterprise Architecture (EA) frameworks, but adds government-specific EA artifacts to account for policy enforcement, and provides guidance for best practice implementation and governance (see Baseline Configuration Standards for more detail).

NITC Enterprise management provides top-down, comprehensive management of the virtualized infrastructure and the applications used to support the environment. The enterprise management layer of midrange services will handle the full system lifecycle of virtualized resources and provide additional common infrastructure elements for service agreement management, monitored usage, configuration management, license management, and optional disaster recovery. The virtual server management software used by NITC allows dynamic provisioning and resource allocation to allow applications to scale on demand and minimize the waste associated with underutilized and static computing resources.

1.1.1.1 Provisioning Standards

NITC will provision virtual machines, logical partitions, and logical domains using supported operating systems. Each server built within the Midrange environment will be dynamic, scalable and virtualized using the operating systems mentioned in

Table 3: Midrange PaaS-Server Resource Configuration Guide.

All servers are designed to interoperate with the most common and up-to-date software development languages and web development technologies.

Appendix A –Midrange

NITC requires customers to submit all new system requests and changes through the Service Desk with workflow for approval through Account Management. NITC will provide customers with resource request templates (through Account Management or the NITC Service Desk) to streamline the process. NITC will also provide guidance to customers during resource requests to be sure that customers are not over-allocating resources. Resources shall be allocated according to the resource allocation schedules in Table 3.

Table 3: Midrange PaaS-Server Resource Configuration Guide

	Resource Configuration Guide				
Operating System	**Minimum(default)**	**Maximum**	**Incremental Allocation**		
	CPU/RAM(GB)/Storage(GB)	**CPU/RAM(GB)/Storage(GB)**	**CPU**	**RAM(GB)**	**Storage(GB)**
Windows™	1/1/50	16/64/950GB	1	.5	Any
Red Hat Linux™	1/1/15	16/64/950GB	1	.5	Any
AIX™	1/3/40	16/64/10TB	1	.5	Any
Solaris™	1/1/50	16/64/10TB	1	.5	Any

Due to NITC policy regarding elevated privileges in Midrange, NITC will require the development of workflow or process to facilitate the deployment of an application into a PaaS server from a customer-owned development or staging server, to ensure proper functionality is maintained and end user acceptance testing is successful. This will allow customers to share information about the application development and testing methods, with the NITC Software Integration Team. NITC will work with the customer to gather and analyze application requirements, for suitability in the PaaS environment, using Enterprise Architecture design methods.

The PaaS-Server environment enables the customer and NITC to control and allocate resources dynamically to meet the changing needs of an application. As application requirements change, NITC will work with customers to alter their solution, as necessary, for performance gains or cost savings. (Note: Given the shared nature of the PaaS-Server environment, the NITC will work, with the customer help, to guide them through proper system sizing in order to save money and avoid underutilized hosting.)

During the integration of customer applications into the NITC architected solution, the customer is solely responsible for investigating licensing requirements and compliance within the NITC PaaS-Server environment. All software is licensed differently and some vendors' licensing schemes may not comply with the PaaS-Server environment.

NITC PaaS-Server architectural design provides an efficient platform for application life cycle management; through the use of development and test, pre-production, and production environments. NITC is required, under NIST 800-53 guidelines, to periodically patch and upgrade operating systems. To retain the Certification and Accreditation, NITC must continuously monitor, upgrade, and patch ALL PaaS-Server operating systems. When customers utilize NITC's PaaS-Server service offering for their production environment ***only***, these patches may be different than those loaded to the development, test, and pre-production environments. The differences in OS levels could adversely affect production application and database environments.

Thus, customers **are encouraged to use** NITC's PaaS-Server service offering for all of their operating environments (i.e. development, test, certification/QA/pre-production, production), to alleviate the risk of potential differences, in the patches, affecting the application life cycle process.

1.1.2 IaaS - Server Hosting Services

IaaS – Server Hosting Services provides a virtual machine infrastructure which allows customers the option to maintain control of their operating and general support systems at the system level. IaaS - Server Hosting Services do not benefit from the same services as a PaaS - Server deployments, IaaS-Server Hosting environment is provided for customers to maintain control of their hosting platform while allowing NITC to control the infrastructure on which it resides. A customer may inherit the necessary infrastructure level controls on which their systems solutions reside. The NITC provides optional additional service attributes to the IaaS – Server similar to the level of service provide in a PaaS – Server offering at the request of the customer. See Table 1: Midrange Services Matrix. Customers may require unique system level dependencies outside of the scope of NITC's standard baseline configuration (as documented in *the Baseline Configuration Standards*). The NITC will work to accommodate those requirements which may require a professional services engagement. The customer will assume the risk in deployment timing, service sustainability, and service reliability in providing IaaS – Server systems with dependencies outside of NITC baseline configuration standards.

1.1.3 Midrange Managed Hosting Services

NITC's Midrange Managed Hosting Service provides customers with the facilities, network, security, and Operating System (OS) system administration required to successfully operate customer owned computer systems. The customer is responsible for hardware purchases, ownership, maintenance, and hardware refresh.

Table 4: Supported Operating Systems for Midrange Managed Hosting Services

	Platform		
Operating System	**X86**	**Sparc™**	**pSeries™**
Windows™	✓		
Red Hat Linux™	✓		
Solaris™	✓	✓	
AIX™			✓

Customers will have full management and administrative authority over their applications. Professional Services are also available to customers using the Managed Hosting Service. The NITC will administer all virtual machines and logical partitions hosted within the customer-provided physical servers. The NITC will build, configure, and maintain all virtual machines and logical partitions according to NITC's baseline configuration standards.

Customers are responsible for their entire system accreditation including the OS; however, NITC will provide OS-level documentation for ST&E submission.

1.1.4 Midrange Collocation Services

NITC's Midrange Collocation Service provides customers with only facilities, physical security, and in the case of "on-network" collocation customers, network security. NITC will not provide any OS administration services to collocation customers.

Unlike the IaaS and Managed Hosting offerings, NITC Professional Services are not available nor are any Disaster Recovery planning or coordination services included. However, NITC Storage Services are available to all Collocation Hosting solutions. NITC will only provide limited Service Desk support. The details on other items included in this service can be found in Table 1: Midrange Services Matrix.

1.1.4.1 ON-NETWORK Collocation Services

Customers who utilize NITC's Collocation services and choose to use NITC's network inherit pieces of the security therein. Systems residing on NITC’s network gain the benefits of added security, but must adhere to all NITC’s network security policies regarding network topology, IP assignment, access controls, etc. Systems residing on NITC networks must also comply with NIST 800-53.

System compliance will be tested on a regular basis. See Section 2.2, “Security Assessment Services (Scanning)”. In addition, many of these items are covered in Section 0 “

1.1.4.2 OFF-NETWORK Collocation Services

Customers who utilize NITC's Collocation services and choose NOT to use NITC's network, but rather deploy or extend their own network will not benefit from NITCs robust network security architecture or many of the other items included in more advanced NITC services. *Table 1: Midrange Services Matrix is not inclusive of OFF-NETWORK customers. While some activities may be included, not all are. For details on OFF-Network activities, please talk to your NITC Account Manager.*

1.1.5 Washington DC Computing Facility Services

To assist USDA in meeting its Federal Data Center Consolidation Initiative requirements, NITC can temporarily host Agency Office Automation Infrastructure (OA) at its Washington, DC (WDC) Computer Room S-100 to allow agency computer rooms to be closed and repurposed. OA is any service, device, or storage that directly supports desktop environments to include network distribution and security services.

On Going Support

While S-100 is for hosting Agency OA only, applications may be allowed to reside in S-100 on a short-term preapproved basis as they are prepared for relocation to KC. The approval process is as follows:

- Agency provides a description of the applications to reside in S-100
- Agency provides a user impact statement if applications are not hosted within S-100

- Agency provides a plan, with completion dates, to modify applications as required to allow for hosting at KC to include dates
- Documents are emailed to the NITC ACIO or DACIO

Within S-100, NITC provides physical security and access in conjunction with Office of Operation's physical security services. NITC also provides space, HVAC, and power.

NITC does not perform backup, offsite storage, network, network security or incident handling, scanning, patching, disaster recovery, etc., services for agency OA located within S-100.

Floor Space

It is the agency's responsibility to supply locking cabinets to house their OA. For the initial installation within the WDC Computer Center, each agency will utilize cabinet space efficiently to minimize the total number of cabinets needed. The agency must provide NITC with cabinet content specifications before installing OA within S-100. Once the agency has completed their S-100 OA installation, all additional equipment installations or space requests must be preapproved by the NITC ACIO or DACIO. S-100 is not intended to be a growth oriented computer room. Agency footprints within S-100 are expected to decrease. S-100 is scheduled to close and be consolidated into the George Washington Carver Center (GWCC) for OA and Kansas City for Business Applications.

NITC performs annual inventory audits of agency OA. Agencies will be notified no less than two weeks prior to each inventory audit as agency assistance will be required.

Appendix A –Midrange

Power

Each agency is responsible for providing Uninterrupted Power Supply (UPS) to meet their uptime requirements. NITC is the single-point-of-contact to the Office of Operations (OO) for all S-100 power requirements.

NITC facilities and engineering staff work with each agency to determine its total S-100 power requirements, along with UPS connectivity and receptacle selection. NITC submits each agency's power requirement into the USDA OO online Building Permit Program System. Once the building permit is approved, an electrician will provide a quote for the electrical work to be completed. NITC will provide a copy of the quote to the agency for reimbursement.

Network Cabling

The agency is responsible for all copper and fiber network cabling within their S-100 located cabinets. For all network connections outside the agency cabinets, the agency must submit a NITC Service Desk request detailing the requirement. Only NITC authorized cable installers may install copper or fiber cabling from agency cabinets to external services. The agency is responsible for directly funding all external cabling requirements. Please refer to section Off-hours and Emergency Support for NITC Server Desk contact information.

S-100 Access

A limited number of agency staff will be provided unescorted access to S-100. S-100 security is configured as follows:

- The main entrance into S-100 is secured via biometrics. Access control lists are managed by NITC and are stored within the Office of Operations Physical Security System.
- WCTS maintains S-100 perimeter access control lists
- The back entrances to S-100 are secured by local alarms and deadbolt locks.
- Cameras are positioned within and outside S-100 and are monitored 24/7 by OO Physical Security.

Unescorted access into S-100 requires, at minimum, a Public Trust clearance level. Agency security officers are responsible for submitting staff member information for unescorted access. All unescorted access requests are to be sent to NITC Physical Security (Contact the NITC Service Desk to be connected with NITC Physical Security staff). NITC manages one access group list for each S-100 located agency.

Off-hours and Emergency Support

Contact the NITC Service Desk. See Appendix L for information.

1.2 Platforms

The following section applies only to Paas-Server Hosting, IaaS Transitional Hosting Services, and Midrange Managed Hosting Services for all platforms, NITC performs administration and maintenance at the hardware and operating system level and the customer is in full control of their deployed applications but also have the option of using NITC professional services for some or all of their application support. For IaaS-Server hosting services, the customer has the responsibility to co-manage the operating system with NITC.

1.2.1 Windows Platform

The Windows Platform provides customers with a fully administered instance of the Microsoft™ Windows© operating system. Systems are deployed according to NITC standards and NIST 800-53 security guidelines. Details on the platform can be found in Section, “System Administration,”

1.2.1.1 Supported Versions (Windows)

The following versions of Microsoft™ Windows© are supported by NITC:

Table 5: Supported Operating System Versions (Windows)

Windows Operating Systems				
OS	Type	Bit Length	Supported on Physical	Supported on Virtual
Windows 2008	Enterprise Edition, R2	64-bit	✓	✓

1.2.2 Linux Platform

The Linux Platform provides customers with a fully administered instance of the Red Hat™ Linux operating system. Systems are deployed according to NITC standards and NIST 800-53 security guidelines. Details on the platform can be found in Section 3, “System Administration,”.

1.2.2.1 Supported Versions (Linux)

The following versions of Red Hat™ Linux are supported by NITC:

Table 6: Supported Operating System Versions (Linux)

Linux Operating Systems					
OS	Type	Version	Bit Length	Supported on Physical	Supported on Virtual
Red Hat Linux	Server	5.x	64-bit	✓	✓
Red Hat Linux	Server	6.x*	64-bit	✓	✓

1.2.3 AIX Platform

The AIX Platform provides customers with a fully managed instance of the IBM™ AIX© operating system. Systems are deployed according to NITC standards and NIST 800-53 security guidelines. Details on the platform can be found in Section 3, "System Administration,".

1.2.3.1 Supported Versions (AIX)

The following versions of IBM™ AIX© are supported by NITC:

Table 7: Supported Operating System Versions (AIX)

AIX Operating Systems				
OS	Version	Bit Length	Supported on Physical	Supported on Virtual
AIX	6.1	64-bit	✓	✓
AIX	7.x**	64-bit	✓	✓

* AIX 5.3 is supported for existing systems, but will only be deployed on new systems with justification and acceptance.

1.2.4 Solaris Platform

The Solaris Platform provides customers with a fully managed instance of Oracle™ Solaris© operating system. Systems are deployed according to NITC standards and NIST 800-53 security guidelines. Details on the platform can be found in Section 3, "System Administration".

1.2.4.1 Supported Versions (Solaris)

The following versions of Oracle™ Solaris© are supported by NITC:

Table 8: Supported Operating System Versions (Solaris)

Solaris Operating Systems				
OS	Version	Bit Length	Supported on Physical	Supported on Virtual
Solaris	10	64-bit	✓	✓
Solaris	11*	64-bit	✓	✓

2 Security

The NITC Systems Security programs provide logical system security controls across the NITC enterprise for the purposes of safeguarding government data, applications, and the operating system. Within the NITC's national enterprise, these programs provide system and data level Role Based Access Controls (RBAC), system risk and threat analysis, and enterprise Public Key Infrastructure (PKI) services. Through the architectural integration of roles, configuration standards, and PKI, access controls are enforced and resilient safeguards established within the data center's hosting environments.

2.1 Midrange System Security Services

NITC provides a highly available centralized authentication, identity management, and role based access control solution. This solution provides user identification, account and role management, and system access provisioning. This system level integration lends data center service support for:

- NITC’s Asset, Configuration, and Change management processes
- Vulnerability detection and remediation management process
- Remote access – multi-factor authentication requirement
- Baseline configuration standards enforcement and monitoring
- Public Key Infrastructure (PKI) integration
- Elevated privilege account controls
- Password management
- User account certification requirements on federal information systems

2.1.1 Central Authentication Solutions

NITC has established a data center authentication solution which supports various authentication protocols for Microsoft, UNIX, Linux, and other hosts using disparate authentication services to include: Lightweight Directory Access Protocol (LDAP), Secure LDAP, Radius, and TACACS. This solution enforces USDA standards for passwords and user’s accounts. This authentication system is integrated and managed by NITC’s Identity Management solution.

2.1.2 Identity Manager

The Identity Manager system provides a Role Based Access Control (RBAC) methodology to separate user access from Elevated Privilege (EP) access. NITC’s Identity Management system uses an established naming standard to identify user accounts from Elevated Privilege accounts. Additionally, NITC certifies user accounts to provisioned roles on a quarterly basis. The Identity Manager uses automated workflow and authorization processes to enforce user account management, role access, and password compliance. This system allows customer security program managers, and their delegated staff members, to manage access to their systems transparently.

On NITC owned and managed service platforms (IaaS, PaaS, and Managed Hosting), The NITC operating system administrator functions as the sole custodian with the highest level of access (e.g. “root” or “admin” authority)

Collocation and Managed Hosting systems are required to integrate with the NITC centralized authentication system through a domain join. This is accomplished using native tools for Windows systems or Agents for Open Systems. There are additional costs associated with the Open Systems Agents that are passed onto the customer.

NITC customers regardless of service level will integrate systems hosted within NITC’s logical network boundaries into NITC’s central authentication, identity manager, PKI, and roles based management solutions.

2.1.3 Elevated Privilege Access Control

The NITC operating system administrator will function as the sole custodian with the highest level of access (e.g. “root” or “admin” authority) for all IaaS – Midrange and Midrange Managed Hosting instances. NITC has implemented a “least privilege” mode of operations, permitting the minimum amount of operability needed to perform mission-essential functions. For some work (typically installation-related activities), this level of access may be extended to customer personnel on the condition that the need for access is requested and documented in advance and is required for only a short duration.

This access will be provided on a temporary basis only and access granted for a predetermined timeframe of no more than 5 business days. All work to be performed during the period of elevated access will be documented by the customer before access is granted and is subject to the NITC's change management procedures. Initiation of elevated privilege access begins with a service request to the NITC Service Desk (See Appendix L). NITC reserves the right to deny access or desired changes if those changes have the potential to affect the security, performance or certification and accreditation of the IaaS environment or if it is determined that said changes could affect another NITC customer. If actions of non-NITC personnel result in an outage, the NITC will analyze and schedule restoration tasks, taking current workload and resource availability into consideration.

2.1.4 Security Baseline Configuration

NITC's baseline configuration standards will be used for all information systems, domain member, application, and database servers. Vulnerability assessment is described in Section 2.2 "Security Assessment Services (Scanning).

2.1.5 Digital Certificates and Multi-Factor Authentication

NITC maintains the data center Public Key Infrastructure solution. NITC supports the use of public digital certificates and costs are passed through to the customer. Additionally, NITC can issue USDA digital certificates upon request as systems are integrated to the data center domain.

NITC integrated the data center domain with the USDA root bridge for USDA LincPass PIV Card capability. The USDA LincPass card is the primary means of Multi-Factor Authentication (MFA). Tokens are available to customers in the event they do not have access to USDA LincPass. There are additional costs passed through to the customer for Tokens. One of the two MFA solutions offered must be used in conjunction with the NITC Remote Access Solution identified in the Network Security Services section in Appendix C. Any elevated privilege access coming into the data center must have a successful user MFA and endpoint host inspection for security purposes.

2.1.6 Enterprise Risks

The NITC reserves the right to remove applications from the Enterprise Network that may pose intolerable risks or eminent threat to the NITC Enterprise Infrastructure or to other NITC customers. Whenever possible, as circumstances or level of threat permit, the NITC will coordinate with the customer prior to removing systems from the Enterprise Network.

2.2 Security Assessment Services (Scanning)

NITC provides host discovery, vulnerability, and compliance scanning services to proactively manage and monitor the health and well-being of systems. Vulnerability scanning activity will inspect the network devices and all assets in the NITC logical network boundaries monthly per USDA requirements. Every device on the NITC enterprise network will undergo an authenticated administrative discovery, vulnerability, and compliance scan using a variety of NITC enterprise tools. Reporting processes are established using the NITC Patch and Vulnerability Management (PVG) process. Hosted systems will be patched or baseline configuration adjustments made as required by NITC standards to avoid the potential service impact. The standard remediation time for high vulnerabilities is immediately but not to exceed 30 days, for medium vulnerabilities, remediation is to occur within 90 days.

Collocation and Managed Hosting customer Security Program Management point of contacts as identified in the NITC Agreement will receive monthly vulnerability reports. NITC system, application, and security administrators are available to assist with remediating systems as it pertains to the customer on NITC owned or managed platforms.

Customer-owned vulnerabilities, defined as application vulnerabilities in PaaS or any vulnerability in Managed Hosting, IaaS or Colocation are required to be remediated in a timely manner to minimize the risk and impact they pose on NITC infrastructure. The NITC provides a vulnerability report to each customer monthly. This report is the first level of notification (vulnerability clock starts). If the same vulnerability shows up on the next month's report (vulnerability is now at least 30 days old) then the NITC ISSPM and NITC DACIO will contact the Customer Agency ISSPM to discuss the issue. If the vulnerability exists on the monthly report following this meeting (meaning the vulnerability is now more than 60 days old) the NITC reserves the right to take mitigating actions on system. Mitigating actions can include (but are not limited to) IPS block, Firewall block, VLAN block, and taking the system offline. The NITC ACIO will make a courtesy call/notification to the USDA CIO and Deputy CIO before action is taken to mitigate the risk. The NITC has a vulnerability waiver process that customers can utilize to document false positives or risk acceptances to prevent specific vulnerabilities from being identified as real risks that need to be mitigated through the escalation process.

2.3 Certification and Accreditation (C&A)

The NITC is responsible for the authorization of controls for its IT General Support Systems (GSSs), Data Center, and centralized IT system solutions (account management, authentication, audit logging, configuration management, and patching). NITC's General Support Systems are interconnected sets of information resources under NITC's direct management control that share common functionality. GSSs include hardware, software, information, data, applications, communications, facilities, and personnel. It is through the authorization of NITC's GSSs that it provides controls to service offerings. The NITC has Authorizations to Operate (ATO) for the NITC Midrange, Mainframe, Network, Infrastructure Support System, and Enterprise Services GSSs.

For IaaS - Midrange Hosting and IaaS – Transitional Hosting services, controls are authorized up through the Operating System as part of the NITC Midrange-GSS. Customers are responsible for the authorization of their applications and databases.

Managed Hosting and Collocation services are under the customer span of management control. Customers are responsible for the authorization of their entire information system, including the application, database, operating system, and hardware. Customers may be able to take advantage of NITC centralized IT system controls, that are authorized by NITC, but only if these controls have been specifically implemented for the customers' system and specified in their NITC agreement.

Controls that are tested and authorized by NITC will not be allowed to be recursively tested by the customer. The NITC will provide copies of the ATO letters for its IT GSSs to the agency/customer Information System Security Program Manager (ISSPM) upon request.

2.3.1 Inheritance of Controls

Due to limitations within the Cyber Security Assessment and Management (CSAM) system, the NITC has modified its approach to inheritance of controls. CSAM only allows NITC to offer controls for inheritance when they are 100 percent provided (implemented, authorized and tested) by NITC. Those controls which are 100 percent provided by NITC, such as physical, environmental, and network controls, are marked inheritable in CSAM within the referenced NITC GSS or Services.

CSAM does not have the ability to mark inheritable controls that are partially provided (hybrid) or shared. ***When NITC is responsible for the operating system controls and the customer is responsible for their application controls, the majority of system controls are either hybrid or shared and the controls are "not inheritable" through CSAM.*** The customer should only select (inherit) these controls for their IT System when they have been specifically implemented for the customers and specified in their NITC agreement.

The NITC will provide separate documents describing control information for those controls that are not inheritable via CSAM. These reports identify the controls that are implemented, authorized, and tested by NITC for its GSSs, services, or centralized IT system solutions.

For Managed Hosting and Collocation customers, NITC will make available documentation about the services provided by NITC that are authorized and tested under the customer's span of management control. These reports will include activity which the NITC performs that the customers can document in their IT System Security Plan (SSP) to illustrate exactly what services they are receiving from NITC.

2.3.2 Interconnection Security Agreements (ISA)

NITC GSS systems that host customer applications do not directly share or exchange data with customer systems. These customer systems are actually running on a NITC General Support System. The Service Level Agreement, task order, and appendices of services along with documents describing the control information meet the requirements for an ISA between both parties.

This documentation provides customers the information necessary to incorporate the services and controls performed by NITC within their System Security Plan and evaluate residual risk for their systems.

3 System Administration

The following section applies only to PaaS- Server, IaaS Transitional Hosting Services, and Midrange Managed Hosting Services. For all platforms, NITC performs administration and maintenance through the operating systems and the customer is in full control of their deployed applications, but has the option of using NITC professional services for any or all of their application support. For IaaS-Server hosting services, the customer has the responsibility to co-manage the operating system with NITC.

The following subsections describe details of NITC's operating system management policies and practices.

3.1 Standard Service Activities

Table 1: Midrange Services Matrix describes common operating system administration activities and defines which service levels include each activity. Some functions included in IaaS services are NOT

included with Managed Hosting. Any activities not listed are assumed to be professional services and should be discussed with NITC Account Management.

3.2 System deployment

The deployment and provisioning of systems, of all types, is initiated by communicating with NITC account managers, gathering requirements and submitting a service request to the NITC Service Desk via standard procedures outlined in Appendix L. Templates for all system resource requests are in place and available through the NITC Service Desk or the customer account managers. Deployment times vary based on the service requested.

3.3 Baseline Configuration Standards

All IaaS and Managed Hosting systems must adhere to NITC’s baseline configuration standards in NIST 800-53 directives for secure systems and NITC specific directives for administration. Table 1: Midrange Services Matrix denotes configuration items required for IaaS and Managed Hosting Customers. Table 9: Baseline Configuration Items outlines the making of a NITC compliant system for all Operating System types.

Appendix A –Midrange

Table 9: Baseline Configuration Items

Compliance
All systems must pass a NITC managed compliance scan. The compliance scans are based off of NIST guidelines. If the candidate does not pass the compliance scans, all findings must be fixed. Any exceptions to the rule must be agreed upon by NITC and its customer and documented accordingly. Furthermore, all candidates must be configured for ongoing compliance tests once accepted into IaaS MR.
This item requires confirmation that Bladelogic is installed on the system and communicating with NITC's Bladelogic System. Following the installation, a compliance check is run and issues addressed.
Removal of Elevated Privileges
In order to assume platform level certification and accreditation, customers will not be allowed to have full elevated privileges (Administrative/Root access) on IaaS MR systems. When elevated access is required, it is addressed on a case-by-case basis and there are provisions for TEMPORARY full administrative access spelled out in the customer Service Level Agreement (SLA).
This item requires a check by NITC compliancy tool (Bladelogic) to confirm that there are not elevated privileges other than NITC staff.
Centralized Logging
All systems must participate in centralized logging for monitoring and auditing purposes.
This item requires a configuration of the archsight agent or syslogd configuration on the candidate and confirmation that log reporting is occurring properly
Centralized Authentication
All systems must be configured to use NITC's Identity Management system with authentication to NITC's directory server. All user access is granted through this access and local system accounts are disallowed.
This item requires domain configuration or Quest Authentication Services agent installation accordingly and confirmation that authentication is functioning properly. This item also requires that all local accounts on the candidate be suspended.
Centralized Patching
All systems must be configured to use NITC's centralized patching system. All systems must adhere to NITC's patch management guidelines and schedules.
This item requires confirmation that Bladelogic is installed on the system and communicating with NITC's Bladelogic System. Following the installation, a patch analysis is run to confirm that the system is at the latest required IaaS MR patch level. If it is not at the proper level, patching must occur prior to acceptance.
Centralized System Management
All systems must participate in NITC's centralized system management system. This assures complete control of IaaS MR systems by NITC operations.
This item requires confirmation that Bladelogic is installed on the system and communicating with NITC's Bladelogic System.
Centralized Vulnerability Scanning
All systems must pass a NITC vulnerability scan prior to deployment into the environment. Furthermore, all systems will participate in routine security scans.
This item requires a request to NITC's Internet Security Branch (ISB) for a security scan on the candidate. Any vulnerabilities that are not standard NITC exceptions shall be addressed prior to acceptance and the system re-scanned.
Centralized Monitoring
All systems must be monitored by NITC's centralized monitoring system.
This item required that the candidate is configured in NITC's centralized monitoring system (Xymon). Any special monitoring requirements or contacts must be agreed upon and configured accordingly.
Participation in Tivoli Endpoint Management (formerly BigFix) reporting
All systems must be configured to the OCIO TEM reporting solution. This is mandated for ALL USDA IT systems.
This item requires confirmation that the TEM agent is properly installed and reporting.
Centralized Antivirus Subscription
All (Windows only) candidates must participate in NITC's centralized antivirus reporting and remediation system.
This item requires confirmation that the IaaS MR (Windows) candidate has the proper NITC sanctioned antivirus software installed and configured to communicate with the centrally managed AV system.
Auto-Discovery participation
All systems must be discoverable by NITC's auto discovery process.
This item requires domain configuration or quest agent installation accordingly and confirmation that authentication is functioning properly. If, for some reason, domain connectivity is not configured for a system, then local credentials for the auto-discovery appliance (ADDM) MUST BE CONFIGURED.

3.4 Operating System Upgrades & Patches

3.4.1.1 Schedule and Coordination with Customer

The NITC will perform operating system upgrades on a periodic basis and in the event of a critical security incident, as ad-hoc deployments for purposes of vulnerability remediation. Customers who utilize NITC for all operating environments (i.e. development, test, certification/QA/pre-production, and production) will have updates applied through all environments using the NITC's Change Management procedures. Customers are notified via email from the NITC Service Desk when upgrades, patching, or system outages are expected to occur.

Note: If a customer is utilizing NITC's IaaS service offering for their production environment only, they run the risk of application or database interoperability issues with the updated operating system.

All UNIX/Linux and Windows-based servers supporting IaaS, PaaS, Managed Hosting, FSA/RD/NRCS WebFarm(s), and NITC-owned internal systems will be patched according to the mandatory standardized, monthly/quarterly reoccurring schedule. See Appendix L for details on Change Management.

3.4.1.2 Official Patch Schedule FY 14

Below is the official combined patch schedule for UNIX/Linux and Windows-based environments at the NITC. The dates on this schedule should not change, however, in the event of a change all customers will be notified by the NITC Service Desk in advance of the dates listed. Please note that some of the dates are adjusted to fit into the federal holiday schedule as determined by OPM.

Table 10: Official Patching Schedule for all UNIX/LINUX and Windows-Based environments

	FY 14	**OS Type**	**DEV/TEST Thursday 15:00-24:00**	**PRE-PROD Tuesday 15:00-24:00**	**PROD Sunday 16:00-02:00**
Q1	Oct-2013	UNIX/Windows	10/17/2013	10/22/2013	10/27/2013
	Nov-2013	UNIX*/Windows	11/21/2013	11/26/2013	12/4/2013
	Dec-2013	UNIX*/Windows	12/12/2013	12/17/2013	12/22/2013
Q2	Jan-2014	UNIX/Windows	1/16/2014	1/21/2013	1/26/2014
	Feb-2014	UNIX*/Windows	2/20/2014	2/25/2014	3/2/2014
	Mar-2014	UNIX*/Windows	3/20/2014	3/25/2014	3/30/2014
Q3	Apr-2014	UNIX/Windows	4/17/2014	4/22/2014	4/27/2014
	May-2014	UNIX*/Windows	5/15/2014	5/20/2014	6/1/2014
	Jun-2014	UNIX*/Windows	6/19/2014	6/24/2014	6/29/2014
Q4	Jul-2014	UNIX/Windows	7/17/2014	7/22/2014	7/27/2014

	Aug-2014	UNIX*/Windows	8/21/2014	8/26/2014	8/31/2014
	Sep-2014	UNIX*/Windows	9/18/2014	9/23/2014	9/28/2014

(UNIX*) NOTE: UNIX systems are patched on a quarterly basis, however, NITC reserves the right to utilize the dates labeled UNIX* to apply emergency security patches to hosts as needed. Customers will be notified prior to utilizing the patching dates for emergency patches purposes.

UNIX/Linux servers are patched in conjunction with windows patching on a mandatory quarterly basis. Server reboots are normally required during quarterly patching activities. These reboots are performed after the installation of patches is complete; customers should expect a brief interruption in service during standard patching activities. A short "burn-in" period follows each environment being patched, to ensure ample customer testing time and to ensure there are no adverse system impacts due to the installation of patches.

As a guideline, patching begins with the development and test environments on the 3rd Thursday of each quarter (January, April, July, and October) between the hours of 1500 and 2400 central time. Pre-Production systems will be patched every 4th Tuesday of each quarter (January, April, July, and October) between the hours of 1500 and 2400 central time, 5 days after dev/test patching is completed. Finally, production environments and any hosts missed during the dev/test window are patched every 4th Sunday of each quarter (January, April, July, and October), 5 days after pre-production patching is completed during the standard maintenance window between 1600 and 0200 central time. **NOTE: See patching table for official patching dates as some dates may have deviated from the described procedure.**

UNIX/Linux servers are patched primarily using scheduled jobs with NITC's standard server automation tools.

3.4.1.3 Windows Patching Procedures

Windows-based servers are patched in conjunction with the UNIX/Linux patching activities on a mandatory monthly basis. Server reboots are normally required during monthly patching activities. These reboots are performed after the installation of patches is complete; customers should expect a brief interruption in service during standard patching activities. A short "burn-in" period follows each environment being patched, to ensure ample customer testing time and to ensure there are no adverse system impacts due to the installation of patches.

As a guideline, patching begins with the development and test environments on the 3rd Thursday of each month, between the hours of 1500 and 2000 central time. Pre-Production systems will be patched every 4th Tuesday of each month, between the hours of 1500 and 2000 central time, 5 days after dev/test patching is completed. Finally, production environments and any hosts missed during the dev/test window are patched every 4th Sunday of each month, 5 days after pre-production patching is completed during the standard maintenance window between 1800 and 2400 central time. NOTE: See patching table for official patching dates as some dates may have deviated from the described procedure.

Windows servers are patched using scheduled jobs through NITC’s standard server automation tools.

3.5 System Backups

System Backups are managed by product offering as described below.

3.5.1 Midrange Managed Hosting Backup Strategies

All Managed Hosting systems utilize NITC’s centralized backup architecture (NetBackup) for system backups unless otherwise requested. See Appendix B for more details.

3.5.2 PaaS Midrange (AIX) Backup Strategies

The AIX environment deploys system backups via IBM’s™ Network Installation Manager (NIM) servers and utilizes the NITC’s traditional backup strategy utilizing a NetBackup client (refer to Appendix B for details) to backup all other system data.

3.5.3 PaaS Midrange (Solaris) Backup Strategies

Utilizes ZFS snapshots in conjunction with NITC’s traditional backup strategy utilizing a NetBackup client (refer to Appendix B for details) to backup all system data.

3.5.4 PaaS Midrange (x86) Backup Strategies

Depending upon the location of the virtual guest in the NITC cloud, backup strategies for x86 systems may be varied. It should be noted that Method 2 below is being phased out over time.

Method 1: The NetApp storage solution for PaaS – x86 (Linux/Windows) utilizes disk-based snapshot technology to create and store point-in-time copies of data that emulate the standard backup and retention policies, this method effectively eliminates the need for traditional backup and recovery services. See Appendix B for details.

Method 2 (phasing out): NetBackup for VMware (NBV) uses a physical server configured as a media server and has a special VMware backup agent installed on it to act as a proxy for the backup of virtual machines without the need for any agents inside the virtual machine. This physical proxy connected to all of the LUNs on the SAN that the VMware hosts see where the virtual machines reside so that it can access the VM’s data. NBV creates virtual machine snapshots and then mounts the VM’s disks to the physical server and then backs this data up across fiber straight to the VTL. NBV has the ability to do file-level restores (currently only for Windows) and full VM restores.

3.6 Audit Logging

All Midrange systems send authentication audit and syslog entries to a centralized NITC syslog server. This allows NITC Security to monitor these logs and certification can occur on a periodic basis. All IaaS systems participate in NITC’s Security Information and Event Management (SIEM) tool. Managed hosting and Collocation systems store these logs locally.

4 Contract Management

4.1 Billing

The NITC will bill the customer on a monthly basis in arrears. After obtaining a user id (the procedure is described at the link below), customers may access the NITC internet based Billing System for usage data and charges and monthly invoice information at https://billing.nitc.usda.gov.

4.2 Procurement

Upon request, NITC will provide procurement services for purchasing software, maintenance, supplies, services, and other components required for operation of the application(s) being hosted by NITC. By utilizing this service, the customer will incur a 5% surcharge.

Requests for procurement services, and project/implementation schedules, must include sufficient lead time to complete those activities required by the Federal Acquisition Regulations, USDA policy, and NITC acquisition procedures, and to allow a minimum of 30 days for delivery of equipment or software.

Procurement requests should be provided in writing to the NITC Customer Account Managers, and should include the applicable Acquisition Approval Request (AAR) number. The customer will need to assist NITC personnel in developing any required supporting documentation, including a statement of work, brand name, or sole source justification, or any other documentation that may be required by the contracting office.

Before any procurement can be completed, the customer will need to execute a new Customer Agreement, or revise an existing Agreement, to provide required funding. The NITC Customer Account Manager will work with the customer to develop or revise an Agreement.

Delays by the customer in obtaining or providing proper approvals, required documentation, or funding **may delay the initiation or completion of procurements, tasks, projects or other service requests.**

5 Disaster Recovery

To protect the NITC's customers in the event of a site-wide catastrophic failure, attack, weather event, or other unforeseen disaster, the NITC has designed, deployed, and tested, a site-wide disaster recovery plan between Kansas City, Missouri and St. Louis Missouri. The implemented architecture allows the NITC to failover systems for customers who have subscribed to NITC disaster recovery services at the NITC alternate facility in St. Louis, Missouri quickly and with as little human intervention as possible.

Customer systems utilizing midrange hosting offerings are eligible to purchase the disaster recovery services from the NITC. Customers will receive many benefits from acquiring disaster recovery with the NITC. Benefits of the recovery architecture include:

- Two disaster recovery exercises per year
- One validation disaster recovery exercise after solution is implemented
- Current Managed Hosting customers with contracted disaster recovery environments located is Beltsville, MD are required to notify the NITC at least 30 days in advance with their exercise request
- Fast disaster failovers (speed of recovery depends on DR model followed)
- No impact on production systems when testing
- Utilizing the NITC disaster recovery services will never require IP address changes
- Generally configuration changes to complex applications and operating systems are not required
- Access to NITC's professional disaster recovery services
- The disaster recovery architecture has been well tested already

The NITC currently offers four unique methods of disaster recovery, including SAN Mirroring, VMware's Site Recovery Manager, Virtual Tape Replication, and Tape Shipping. These methods of disaster recovery are outlined in the following sections.

5.1 The Heart of Disaster Recovery at the NITC

5.1.1 HA Core Network

The redundant core network solution is the base of the disaster recovery infrastructure and guides the entire design and recovery process. The core network configuration is made up of several components. Each component has a specific configuration duplicated in both Kansas City and St. Louis:

- Universal Telecommunications Network (UTN): Edge routers
- Perimeter: Firewalls
- Core: Routing
- Distribution: VLANs

Each component above in Kansas City is duplicated in St. Louis. The configurations of each layer are either replicated or restored in the event of a disaster or exercise. These unique features allow the NITC to offer a disaster recovery solution for customers that require no IP address changes or other complicated changes to customer environments.

5.1.2 Access Layer

The access layer is the connection point for all computing devices. This layer is composed of one major component:

- Access Layer: Switches

5.1.3 Storage Services Layer

The storage services layer of the NITC disaster recovery environment manages the way that the NITC stores and recovers data. The storage services layer consists of the following services:

- Storage Network (switches/cabling)
- SAN/NAS Disk Subsystems
- Physical and Virtual Tape Libraries
- Backup Network
- NetBackup Services

Just like the HA Core Network components, each component of the Storage Services Layer in Kansas City is duplicated in St. Louis. The configurations of each layer are either replicated or restored in the event of a disaster or exercise. These unique features allow the NITC to offer a disaster recovery solution for customers that require no IP address changes or other complicated changes.

5.2 How the NITC DR Solution Works

5.2.1 Technical Summary

The NITC network in Kansas City has an EXACT duplicate in St. Louis. The duplicated network is in what NITC refers to as a Dark configuration. In other words the dark network is isolated and blocked off from any and all external traffic, except through a single remote access method. This duplication includes all devices defined in the NITC HA Core Network and Access Layers described above. There is also a live component of the NITC network in St. Louis that houses active systems that do not participate in the "dark" disaster recovery exercises, but do participate in real disaster recovery scenarios.

The NITC storage area network is also comprised of selectively duplicated systems to the St. Louis disaster recovery facility. This includes such things as hardware, software, and most importantly customer data, whether on disk or tape storage. The items duplicated are listed in the Storage Services Layer defined above. The mirrored disk and tape data is crucial to the success of this disaster recovery scenario.

IaaS systems using NITC cloud hardware in Kansas City, that have chosen to participate in disaster recovery, are automatically mirrored and recovered to NITC facilities in St. Louis. This is either done with Site Recovery Manager (SRM), in the case of our VMware cloud, or with SAN mirroring, in the case of NITC other IaaS cloud offerings (AIX/Solaris). Systems are brought online with the exact operating system and data that they had in Kansas City and even on the same IP address. This type of failover results in very quick recovery and minimal downtime.

5.2.2 Five General Steps to a Disaster Recovery Exercise at the NITC

1. ***Network*** - Network at recovery site is activated
2. ***Enterprise Storage*** - Shadow image copies are suspended either manually or by running scripts
3. ***Enterprise Storage Management*** - Backup management servers are brought online by Open Systems administrators
4. ***Auxiliary Support Systems*** - All Auxiliary support systems (virtual/physical) are brought online by systems group
5. ***Customer Recovery*** - Systems and application recovery procedures are employed based on assigned customer priorities

5.2.3 Seven Steps to a True Disaster Recovery

1. ***UTN*** – KC traffic is redirected to St. Louis once NTSO makes route configuration changes
2. ***Network*** – Network at recovery site is activated
3. ***Network Security*** – Information Systems Security Branch (ISSB) performs Firewall configuration changes
4. ***Enterprise Storage*** - Shadow image copies are suspended either manually or by running scripts
5. ***Enterprise Storage Management*** - Backup management servers are brought online by Open Systems administrators
6. ***Auxiliary Support Systems*** - All Auxiliary support systems (virtual/physical) are brought online by systems group
7. ***Customer Recovery*** - Systems and application recovery procedures are employed based on assigned customer priorities

5.2.4 Other Technical Considerations

Customers wishing to run database systems under IaaS services at the NITC should plan on multiple recovery methods. Recovery of an active database has inherent risks with data in flight. Database recoveries should not be allowed to rely solely on SAN mirroring. In addition to mirroring data customers should utilize vendor specific backup techniques in the event that mirrored data is not consistent. Database recovery techniques need to be used to bring up recovered databases. *Customers should not expect active databases to immediately start upon activation of their running system.*

5.3 Disaster Recovery Testing

NITC Contingency Management will schedule and coordinate annual exercises for midrange customers subscribing to disaster recovery hosting services on IaaS and Managed Hosting services, at the NITC's disaster recovery facility. All customers will test at the same time during a disaster recovery exercise to mimic an actual disaster situation. Prior to any testing, the customers will be required to provide their disaster recovery test objectives to the NITC contingency management staff. For further information, see Appendix K on Professional Service Support for disaster recovery planning.

NITC Disaster Recovery planning and coordination services of NITC resources are included as part of all IaaS and Midrange Hosting solutions. For solutions that include a hosted disaster recovery solution in another NITC-managed facility, coordination of annual functional disaster recovery testing is included.

At the initial implementation of disaster recovery services, the NITC does allow for ad-hoc testing of the services being provided. These ad-hoc tests can be scheduled with an account manager and scheduled for a time that fits with both the NITC and the customer's timeline. Other than the initial implementation of disaster recovery services, ad-hoc testing is not permitted, except on a case by case basis. Contact your account manager for more information.

The disaster recovery solution does not support reconstitution of data back to the primary site during or after testing. Customer testing plans should account for the ability to leave production sites up at the primary location during testing and deleting the test copy when testing is completed. Running production at the disaster recovery site as a test is not supported.

5.4 Declaring a Disaster

Disasters shall be declared exclusively by the NITC, as a disaster is defined as a site-wide event. The NITC Service Desk and management will communicate events of this nature directly to our customers via phone and email. It should be noted that Disaster Recovery as defined by the NITC is complete site failover, not simply backup and recovery. Disaster Recovery is not a substitute for Highly Available systems. Backup and Recovery documentation is found in Appendix B.

5.5 Available Disaster Recovery Methods

The NITC's flexible disaster recovery architecture allows our customers to choose between any one or a combination of the following disaster recovery methods. It is possible to employ several of the recovery methods listed in Table 10 as an additional safeguard. For instance, a customer could choose to use SAN Mirroring and for extra protection choose to use Virtual Tape Replication as well. Should the SAN Mirroring not recover as expected, the customer will have a fallback in the use of Virtual Tape at the recovery site.

Table 10: Recovery Methods by Service Offering

Recovery Method	NITC Service Offering			
	PaaS Server	IaaS Server	Midrange Hosting	Collocation - On/Off NITC Networks
SAN Mirroring	✓	$	✓	✓
Site Recovery Manager*	✓	$		
Virtual Tape Replication	✓	$	✓	✓
Tape Shipping**				

*Site Recovery Manager is available for VMware IaaS and PaaS customers only (Linux/Windows)

** Tape Shipping is planned but currently unavailable to our primary DR facility in St. Louis, Missouri.

5.5.1 SAN Mirroring

NITC's SAN replication infrastructure is the primary basis (for services outside of IaaS & PaaS Windows/Linux) of the St. Louis disaster recovery solution. All Kansas City SAN-attached customers have the option of subscribing to SAN replication to St. Louis. As is the standard, the primary disk (in Kansas City) is replicated to a geographically diverse facility, establishing a secondary copy in St. Louis (HUR copy); the secondary copy is locally replicated to a tertiary copy (ShadowImage copy)—this tertiary copy is the copy used during disaster recovery exercises and actual disasters.

5.5.2 VMware's Site Recovery Manager

For customer's using the NITC's Intel IaaS service offerings, VMware's Site Recovery Manager (SRM) product automates the entire system definition and disaster recovery process. With SRM, the primary VMware system in Kansas City is paired to an alternate VMware system in St. Louis. SRM defines both the source and target virtual guests on the primary and alternate VMware systems; additionally, SRM defines the order of virtual guest recovery.

In the event of a DR exercise (or a true disaster), the VMware team will execute the recovery procedure bringing the primary guests online at the alternate site in the St. Louis DR Dark network zone; the alternate systems will be identical to the production systems in Kansas City. No network changes to the guest OS or the application configuration are required by the NITC or the customer!

5.5.3 Disk Based Backup Strategy

Backups stored in Kansas City will be geographically replicated to St. Louis for all customers that subscribe to Enterprise Storage Services. St. Louis will become the offsite storage facility for all customers regardless of hosting subscription as long as they subscribe to Enterprise Storage Services—in the event of a true disaster or a recovery exercise, all offsite volumes will be available at St. Louis. This offsite storage serves as an alternate recovery method to data mirroring..

5.5.4 Tape Shipping (Virtual and Physical)

Shipping tapes from Kansas City, Missouri to St. Louis, Missouri is currently unavailable for our midrange customers, but is a planned offering. Customers will be updated when the option becomes available.

5.5.5 Recommended Disaster Recovery Methods by Service Offering

- **PaaS - Linux (VMware)**
  - Site Recovery Manager
- **PaaS - Windows (VMware)**
  - Site Recovery Manager
- **PaaS – AIX**
  - SAN Mirroring (hybrid)
- **PaaS – Solaris**
  - SAN Mirroring (hybrid)
- **Midrange Hosting - Linux (Physical system)**
  - HDS HUR SAN mirroring
  - VTL replicated tape
- **Midrange Hosting - Windows (Physical system)**
  - HDS HUR SAN mirroring
  - VTL replicated tape

- **Midrange Hosting and PaaS - UNIX (AIX/Solaris)**
  - HDS HUR SAN mirroring
  - VTL replicated tape

5.6 Professional Services

The NITC offers professional services for disaster recovery for IaaS and Midrange hosting customers. Contact your account manager for more information.

5.7 Disaster Recovery Costs

Disaster recovery can be quite expensive, especially when combining primary and secondary methods of recovery as a safeguard. Careful consideration should be given to Recovery Time Objective (RTO) and Recovery Time Objective (RPO) calculations. In addition, customers should give consideration to excluding environments for disaster recovery. For instance, customers may only need to recover production environments in a disaster.

Table 11 shows a relative cost comparison of the different recovery methods.

Table 11: Comparison of Disaster Recovery Costs by Recovery Method

Recovery Method	RTO**	Cost Comparison
SAN Mirroring	4 hours	$$$
Site Recovery Manager*	4 hours	$$
Virtual Tape Replication	24 hours	$$
Tape Shipping***	72 hours	$

*Site Recovery Manager is available for VMware IaaS and PaaS customers only (Linux/Windows)

**Recovery Time Objectives are only given as estimates; actual conditions may result in shorter or longer recovery times.

*** Tape Shipping is planned but currently unavailable to our primary DR facility in St. Louis, Missouri.

Example Scenario: Customer is subscribing to IaaS and has multiple environments at the NITC, and would like to have disaster recovery options for all environments.

Table 12: Example of DR Methods based on Environment

Environment	Recovery Method	RTO	Cost Comparison
Production	Site Recovery Manager	4 hours	$$
Development	Virtual Tape Replication	24 hours	$$
Test	Tape Shipping	72 hours	$

5.8 Disaster Recovery Roles and Responsibilities

Table 113 gives an explanation of what customers can expect during disaster recovery exercises and real disaster recovery situations.

Table 1113: DR Roles and Responsibilities

NITC Service Offerings	NITC Disaster Recovery Roles and Responsibilities				
	Infrastructure Recovery	Auxiliary Systems Recovery	Hardware Recovery	Operating System Recovery	Application Recovery
PaaS-Server	NITC	NITC	NITC	NITC	Customer
IaaS Transitional	N/A		N/A	N/A	N/A
Midrange Hosting	NITC	NITC	NITC/Customer	NITC	Customer
Collocation (on NITC network)	NITC	NITC	Customer	Customer	Customer
Collocation (off NITC network)	Customer	NITC	Customer	Customer	Customer

6 Midrange Services Roles and Responsibilities

Systems Administration and Support Services	NITC Admin	NITC or Customer Admin	Customer Admin
Definition of technical requirements (software, storage, database, disaster recovery, etc.)			✓
Solution proposal based on defined technical requirements	✓		
Procurement and technology refresh of hardware infrastructure/components	✓		
Procurement of virtual Operating System licenses		✓	
Certification and Accreditation (C&A) of the IaaS environment		✓	
Security Testing and Evaluation (ST&E) of the IaaS environment		✓	
Development and maintenance of documentation for IaaS infrastructure, configuration, and operating procedures	✓		
Design, installation, maintenance, and support of the hardware platform	✓		
Design, installation, and support of hardware upgrades and technology refresh	✓		
Design, installation, maintenance and support of the operating system	✓		
Perform operating system hardening, patching, and upgrades		✓	
Monthly Operating System Compliance Scanning and remediation		✓	
Customer validation testing related to OS changes, maintenance activities, and upgrades			✓
Monitoring of server utilization and availability (Operating System)		✓	
Server-side storage administration and management		✓	
Operating System patching and vulnerability management		✓	
Implementation of system changes required to correct performance issues		✓	

SAN/NAS Storage Services	NITC Admin	NITC or Customer Admin	Customer Admin
Procurement and technology refresh of the SAN/NAS storage infrastructure/components	✓		
Design, installation, maintenance and support of the SAN/NAS storage infrastructure	✓		
Installation and maintenance of any required Host Bus Adapters (HBAs)	✓		
Installation of fibre cable to meet any SAN connectivity requirements	✓		
Identification of disk storage and replication requirements	✓	✓	✓
Configuration of SAN/NAS disk storage to meet identified requirements	✓		
Monitoring and operation of local and remote disk storage replication	✓		
NITC data migration to support performance management and technology refresh	✓		
Troubleshoot perceived I/O performance issues	✓	✓	✓

Application and Database Administration and Support Services	NITC Admin	NITC or Customer Admin	Customer Admin
Determination of application/database licensing needs and compliance in IaaS environment			✓
Installation, maintenance, and upgrades of application/database and related components (non-privileged)		✓	
Installation, maintenance, and upgrades of application/database and related components (privileged)	✓		
Application and Database administration and management		✓	
Requisition of system level Database Administration changes			✓
Review and implementation of system level database changes		✓	
Application and database patching and vulnerability management		✓	
Requisition of application and database deployments and upgrades			✓
Release management and implementation of deployments and upgrades		✓	
Implementation of application changes required to correct performance issues			✓
Application and database change validation testing			✓
Load, stress, and validation testing		✓	✓
Application and Database component monitoring		✓	
Application and Database component custom monitoring test creation		✓	✓

Appendix A –Midrange

Network/Security Services	NITC Admin	NITC or Customer Admin	Customer Admin
Procurement and technology refresh of network infrastructure/components	✓		
Design, installation, maintenance and support of the physical and logical network infrastructure	✓		
Public and Private IP address assignment	✓		
VLAN assignment including tiered application services (e.g. Web, Application, Database and etc.)	✓		
IP address routing development, implementation, maintenance and support	✓		
NAT assignment and configuration for Private IP addressing	✓		
Firewall Service Module(FWSM)/Access Control List (ACL) configuration, implementation, maintenance and support	✓		
EtherChannel/VLAN trunking design, implementation, maintenance and support	✓		
DNS support for URL creation, maintenance, and changes	✓		
Network Load Balancing design, implementation, maintenance, and support	✓		
Network infrastructure troubleshooting including packet captures and analysis	✓		
Network infrastructure availability and performance monitoring	✓		
Monthly vulnerability scanning and reporting	✓		
DNS entries/URL creation			✓
HTTPS certificate requests and installation	✓		
Identify firewall configuration changes to support application requirements	✓	✓	✓
Implement and maintain firewall configuration changes to support identified requirements	✓		
Identify remote elevated privilege access requirements			✓
Implement and support identified remote access requirements	✓		

Data Backup and Recovery Services	NITC Admin	NITC or Customer Admin	Customer Admin
Procurement and technology refresh of the backup infrastructure/components	✓		
Design, installation, maintenance and support of the backup infrastructure	✓		
Installation, configuration, and maintenance of standardized IaaS backup solution	✓		
Install and configure backup software to support non-standard backup data retention requirements	✓		
Administration of automated backup policies and schedules	✓		
Troubleshooting of backup processing failures or suspected performance issues	✓	✓	✓
Implementation of server-side changes required to correct backup processing issues	✓		
Implementation of application-side changes required to correct backup processing issues		✓	
Plan and configure application or database level backup/recovery processes	✓		✓

Helpdesk Support Services	NITC Admin	NITC or Customer Admin	Customer Admin
Notifications of incidents and planned infrastructure maintenance activities	✓		
Service Request Submission			✓
Service Request Tracking	✓		

* NITC performs these responsibilities as part of optional Application Integration and Database Administration Professional Services

UNITED STATES DEPARTMENT OF AGRICULTURE

NATIONAL INFORMATION TECHNOLOGY CENTER (NITC)

Appendix E – PaaS Mainframe

Mainframe Platform as a Service

FY2014

The Mainframe Platform as a Service provides a robust, fully-managed enterprise datacenter infrastructure to enable rapid zOS-based application development and deployment.

Table of Contents

1 Introduction 3
2 System Administration and Support Services 3
2.1 System Administration Provide on-site technical expertise to: 3
2.2 Applications/Database Management 6
3 Daily and weekly backups to tape 7
3.1 Backup activities include the following: 7
3.2 Storage management activities include: 7
4 Procurement Services 9
5 Facility security 10
6 Cyber Security 11
7 Disaster Recovery 13
7.1 Disaster Recovery (DR) Service Quality Targets (SQTs): 14
7.2 Customer Disaster Recovery Responsibilities 16
8 Data Center Facility 16
8.1 Server availability 24 hours a day, 7 days a week 16
8.2 USDA WAN connectivity 17
8.3 Internet Intrusion Detection/Vulnerability Assessment 18
8.4 NITC Service Desk 18
9 Notification of anticipated downtime 18
10 Notification of system failure 19
10.1 System outage logs 19
11 Billing 19

MAINFRAME PLATFORM AS A SERVICE

1 Introduction

The NITC Platform as a Service (PaaS) Mainframe environment supports consolidation and virtualization through the sharing of resource pools. This environment assures scalability to respond to the dynamic demands of applications, resulting in optimal utilization of resources. The ability to balance workloads from a mix of applications helps normalize system utilization and reduces the extent of the variations between peaks and valleys. In this environment costs are allocated based on resource usage, rather than resource availability. The enterprise environment is maintained as a complete system where new technology is introduced as it becomes available on a regular basis. Systems engineering, performance tuning and monitoring are continuously performed to provide near 100% scheduled availability.

2 System Administration and Support Services

The System z mainframe server environment provides a hardware platform that enables the sharing of resources. NITC provides system administration to assure customer production work environments are implemented and customized to provide the requested production job utilization and performance priorities. Adjusting the priorities and workload requirement are part of mainframes inherent ability to respond to the dynamic demands of applications, and provides the resultant optimization of resources. The mainframe reliability comes from the ability to customize and standardize customer workloads, while balancing the mix of applications and reducing the extent of the variations during times of high and low demand.

In this environment costs are allocated based on resource usage. NITC system administrators perform scheduled maintenance during established scheduled maintenance windows. The enterprise environment is maintained as a complete system where new technology is introduced on a regular basis. Systems engineering, performance tuning and monitoring are continuously performed to provide near 100% scheduled availability.

2.1 System Administration Provide on-site technical expertise to:

- Install/upgrade mainframe operating system
- Install and maintain mainframe COTS software
- Perform scheduled maintenance
- Troubleshoot operating system and COTS software production issues
- Define and maintain hardware configuration
- Monitor and control systems
- Perform production control

Table 1 describes task descriptions for each of the above listed activities.

Table 1: System Administration

Activity	Tasks/Description
Install / upgrade mainframe operating system	• Acquire disk volumes • Create disk volume names • Select options to install • Generate install jobs • Set-up licensing keys • Run process to validate completion of install • Execute/install scripts/jobs • Execute Initial Program Load (IPL)- verify stable operating system • Install customizations/run-time options (SORT, TSO, etc.) • Clone operating system to LPARs • Customize operating system for each dedicated mainframe environment • Maintain automated operations, software and documentation
Troubleshoot operating system and COTS software production issues	• Field calls from customer/SNCC • Receive/initiate problem report • Investigate and analyze problems (SNCC monitors) • Research fixes • Recommend solutions (SNCC monitors) • Cancel/kill jobs • Modify system/COTS software options • Initiate dump data set for diagnostics • Forward to responsible party for fix • Initiate Severity "Sev-1" • Create change, incident and problem record documents • Identify, install, migrate, clone fix
Define and maintain hardware configuration	• Determine peripheral hardware needs (printers, disks, tapes, front-end processors) • Define open system adapters (IP) • Define infrastructure (tape subsystems) • Establish addresses

Activity	Tasks/Description
Install and maintain mainframe COTS software including: Utilities Data Storage Products Teleprocessing Software Language Compilers and Related Products Database Management System Software Web Services Software and Tools Data Warehouse Software and Tools Transaction Processing Software Automated Schedulers & Production Control Sys Telecommunications Subsystems and Protocols Decision Support Software Office Automation Software Text Processing Software Statistical Packages Executive Information System Software Human Resource Management Software Computer-Based Training	• Customize configuration • Apply/acquire licensing keys • Create CLISTS and PROCS • Update/customize PARM LIBS • Test software to validate installations • Unload tapes • Set-up JCL • Execute program/install JCL • Apply PTFs • Coordinate with customer/NITC personnel • Follow installation IRT standards, change records • Move software to production
Perform scheduled maintenance	• Perform Initial Program Load (IPL) • Establish priorities for processing (logical partition) • Modify LPAR configuration • Schedule downtime for upgrades, cleaning, testing power, adding equipment • Coordinate schedule with affected parties
Monitor and control systems	• Monitor systems response time • Analyze system availability • Monitor system performance • Adjust production control • Monitor loads • Monitor system performance
Perform production control	• Schedule jobs • Job completion codes • Analyze for abnormal endings • Report status of processing • Provide support for workload automation (scheduling, automatic restart, etc.) • Control Mid-Range production • Maintain queue • Contact customer for rescheduling

2.2 Applications/Database Management

Provide on-site technical expertise to:

- Install/upgrade database/application/server releases
- Maintain and administer databases and applications
- Support applications
- Troubleshoot database and application problems

Table 2: System Administration

Activity	Tasks/Description
Install/upgrade database/application/server releases	• Receive software media • Create JCL scripts • Mount tapes • Configure server • Load software • Create DB instance • Test features and components • Determine number of DB instances (spread) • Load/define/install/spread database • Migrate to production • Migrate existing configuration/data between versions • Training/support/test tools • Upgrade to new versions • Perform regression testing • Test new features • Update log to reflect number of DB instances
Maintain and administer databases and applications	• Analyze and monitor system performance issues • Manage user groups o Perform set-up o Grant permissions o Analyze processing o Process Queries o Create JCL • Build database o Create tables o Debug design issues o Redesign o Compile customer applications • Perform scheduled maintenance • Perform proactive maintenance • Research Programmed Temporary Fixes (PTF)'s • Report issues to vendors

Activity	Tasks/Description
Support applications	• Write installation procedures • Mail install instructions/CD's • Support customer with install via phone • Assist with general query • Train customer • Install patches
Troubleshoot database and application problems	• Receive customer inquiry/NITC staff inquiry • Investigate failure • Coordinate with other branches • Create problem report • Create change record Installation Review Team (IRT)/ Midrange Installation Review Team (MIRT) records • Identify fix • Get approval for fix • Resolve problems

3 Daily and weekly backups to tape

Data management procedures for the project will include daily and weekly backups. Multiple sets of backup tapes will be maintained and cycled through an on-site tape library as well as an off-site storage facility. The off-site storage will be provided through NITC's contracted provider.

3.1 Backup activities include the following:

- Incremental backups: Backups of new or updated DASD datasets are taken nightly. Backup tapes are kept on-site in the tape library.
- Weekly/monthly full volume backups: Backups of all DASD volumes are accomplished on a weekly and/or monthly basis. (Retention for monthly backups is longer.) Full volume backups are used at the NITC and are kept off-site (but can be recalled whenever needed).
- ABARS backups: IBM's Aggregate Backup and Recovery Support (ABARS) software was selected by the NITC for disaster backup and recovery. The NITC's customers assume responsibility for determining the applications saved and the frequency of these backups.

3.2 Storage management activities include:

- Design storage structure
- Manage storage system and data availability
- Administer and maintain storage system
- Troubleshoot storage system and network
- Upgrade storage system
- Manage and control tape library

Table 3: Storage Management

Activity	Tasks/Description
Design storage structure	• Determine storage groups • Design physical structure of data • Determine storage requirements (data set size, etc.) o Scope size of system o Determine business needs (back-up, hardware and software management tools) o Performance monitoring and storage monitoring tools • Determine accessibility, availability, migration schedule • Create PACS (primary and hotsite) • Establish Storage Management Subsystem (SMS) constructs • Analyze interoperability of software, hardware, firmware, operating system
Manage storage system and data availability	• Perform system back-up • Perform incremental data back-ups (tape) • Perform full volume back-up • ABARS • Restore site • Back-up operating system • Create lists of data sets • Establish naming convention
Administer and maintain storage system	• Install and maintain storage products • Placement of data sets • Restore data sets • Migrate to Level II • Compress tapes • Evaluate clean-up (administrative) processes • Determine hierarchy (Level II tape) • Manage space allocation • Set/reset thresholds • Add volumes as needed • Determine where to store (offsite/onsite) - Product reports • Respond to warning messages • Direct data set placement to virtual tape, DASD, etc. • Monitor performance/traffic • Adjust data flow • Monitor fibre switches • Monitor Tape Library • Perform LUN security • Track modifications • Assign disk space

Activity	Tasks/Description
Troubleshoot storage system and network	• Receive inquiry from customer/customer representative/system administrator • Create change record • Investigate and analyze problems • Research fixes • Recommend solutions • Modify system options • Forward to responsible party for fix
Upgrade storage system	• Migrate data from old to new • Define devices • Initiate structure
Manage and control tape library	• Mount tapes • Create schedule (pull-list) • Set-up JCL • Run jobs • Install, order, upgrade, certify automated tape mount display system • Notify responsible party for repairs • Schedule maintenance • Control inventory • Order new inventory • Manage offsite storage program • Send out tapes • Create backup tapes on regular basis • Ship, receive, store tapes • Report/analyze physical tape assets • Administer tape library • Follow and maintain IRT/MIRT procedures

4 Procurement Services

NITC can provide procurement assistance for additional specialized software that is not provided as part of the service. In addition to the software acquisition cost a 5% service fee will be applied for the acquisition of any customer-specific software.

Table 4: Procurements

Activity	Tasks/Description
Execute acquisitions and procurements	• Receive purchase inquiry from customer or internal staff • Determine value of procurement • Define requirements (hardware, software, support services, maintenance, etc.) • Conduct market research/prepare RFI/evaluate products • Write waiver request for approval to buy technology • Prepare funding document (AD-700) • Write Statement of Work (SOW) • Buy goods/services
Administer contracts	• Monitor contractual obligations and performance • Verify contract terms are met • Approve invoices • Perform COR/COTR duties • Renew contracts • Enforce compliance • Maintain support contracts • Upgrade software license • Coordinate hardware/software maintenance services
Evaluate proposals	• Prepare RFQ/RFP • Evaluate technical proposals • Evaluate financial cost proposals • Make award recommendation
Develop/write proposals	• Develop work plan • Develop technical solution and alternatives • Develop pricing estimate • Determine operational requirements (security, telecom, etc.) • Analyze opportunity • Determine scope • Maintain client relationship • Make go/no go decisions on opportunity • Facilitate through approval process

5 Facility security

Secure access to the equipment. The controlled environment that NITC provides includes climate control, dual source fire protection, fire alarms, and water alarms. Additionally, the building is protected with closed circuit TVs. Gated entry and security walls surround the facility and control access to the building. Guards are posted at every door and periodically perform roving patrol of the parking lot. Biometric card readers control access to the computer room, as well as the office areas.

6 Cyber Security

The System z mainframe server environment provides a hardware and OS platform which maintains customer separation meanwhile enables the sharing of resources. NITC provides security administration on the platform to assure customer production work environments are implemented and customized based on security role based requirements. The strength of the security administration service implementation is the integration of the least privilege access model. In user appropriate roles, personnel have access to perform their functions only within their customer enclave to maintain a separation of duty. Designated customer security officers maintain system rights to perform account management and access controls over users and applications within their span of management.

The NITC Security Administrators provide a comprehensive security application administration for the z/OS resources across the operating system, subsystems, and OEM software and database components. Additionally, they monitor access violations, assist agency security officers, and implement system software updates during schedules mainframe maintenance windows.

Depending on customer requirements, NITC provides two environments with Access Controls; ACF2 and RACF. ACF2 (more formally, CA-ACF2; the ACF stands for Access Control Facility) is a set of programs from Computer Associates that enable security on mainframes.

The Mainframe Security Architecture is a decentralized model where each agency has scoped authority allowing the decentralized administrators to perform administration within their agency. Agency Security Officers maintain their Data Set Rules while all Resource Rules are maintained by NITC mainframe Security Officers.

RACF, short for Resource Access Control Facility, is an IBM software product. It is a security system that provides access control and auditing functionality for the z/OS and z/VM operating systems.

Each security system supports the following features:

- Identification and verification of a user via user id and password check (authentication)
- Identification, classification and protection of system resources
- Maintenance of access rights to protected resources (authorization)
- Control the means of access to protected resources
- Logging of accesses to a protected system and protected resources (auditing)
- Allows vendor products and applications to interface with Security System controls and features.
- Digital certificates/public key infrastructure
- LDAP & CICS interfaces
- Extensive reporting options, online monitoring and automatic logging capabilities

Table 6: Systems Security Activity	**Tasks/Description**
Install/configure/administer/monitor security hardware/software	• Install administer security cryptographic master key • Install/manage/maintain security products • Add privileged users, establish passwords, and control access • Review and clean up role and resource access rules not used • Install/configure/administer/monitor OS access • Document install/configuration • Monitor security hardware/software • Manage digital certificates (PKI- Secure Socket Layer (SSL))
Develop/create/maintain security program	• Assess risks • Certify processes • Perform security tests and evaluation (ST&E) • Report to external entities (OMB, GAO, GISRA) • Create/maintain COOP and DR plans for security applications • Establish, monitor and oversee security requirements/policy • Direct security awareness programs • Provide security training and education

7 Disaster Recovery

The NITC provides DR services, schedules annual DR exercises, and work closely with the customer for all hardware and services modifications. The NITC also maintains a current DR plan for its data center and will develop and maintain recovery procedures for the customer system environment.

In a disaster scenario, the NITC concurrently restores software and data (including operating system software, utilities, database software, and mainframe customer data) and the backbone communications network within 24 hours from declaration of a disaster. When this task is complete, customers are given access to the hot site computer system to recover selected applications that have been previously backed up and taken to the off-site location for storage. The NITC personnel are available through the duration of the recovery to assist customers in restoration of systems and data.

The NITC assumes responsibility for providing the capability to restore the baseline system, which consists of the operating system, the commercial off the shelf (COTS) software, customer data hosted on the mainframe, and access to the USDA network. To provide this capability, NITC continuously mirrors mainframe data from our primary location in Kansas City, MO to an alternate Disaster Recovery site located in St. Louis, MO.

Customers assume the responsibility of restoring their application data, program library, and all files associated with the application, and is, therefore, responsible for ensuring that their application data and libraries are backed up. NITC uses IBM's Aggregate Backup and Recovery Support (ABARS) software for customer specific disaster backup and recovery.

In a disaster, after the NITC has recovered the baseline system, customers will be given access to the system to restore their application. The NITC personnel will be available through the duration of the recovery to assist customers in restoration of systems and data.

The NITC conducts annual disaster recovery exercises to test its recovery process. The testing includes restoring the system using a mirrored copy. Customers will participate in the exercises by testing their ability to restore their applications. An effort will be made to avoid scheduling the exercises during any customer's peak processing periods. NITC will provide the results of these exercises to the customers.

In a disaster that requires moving processing capability to the alternate site, customers will be responsible for providing connectivity.

The NITC Security Staff coordinates all disaster recovery issues and maintains a detailed disaster recovery plan related to the general support system (GSS).

Activities provided include the following:

- Conduct disaster recovery
- Establish and maintain disaster recovery plans

Table 6: Disaster Recovery

Activity	**Tasks/Description**
Conduct disaster recovery	• Execute disaster recovery plan • Prepare, perform and maintain back-ups • Conduct disaster drills • Request tapes and assess conditions • Create data back-up list (determine which tapes to pull) • Analyze data sets to determine how things are brought back • Reconnect telecommunications • Bring up systems (databases, operating system) • Document activities
Establish and maintain disaster recovery plans	• Develop and maintain contingency/disaster recovery plans • Determine hardware requirements (tape drives needed) • Review and update documentation • Ship tapes • Recommend disaster recovery solutions and techniques to customer

7.1 Disaster Recovery (DR) Service Quality Targets (SQTs):

NITC has developed a set of services quality targets to define the responsive steps and measurements required to make informed decisions upon recovery strategies and the method and timing of reporting.

Table 7: Disaster Recovery Service Quality Targets

SQT	SQT Definition	SQT Metric	Measurement & Reporting	Comment/Assumption
24 Hour Restoration	Severity 0 Response	• Immediate response • Production Environment: Recovery time objective (RTO) of 12 hours of data center restoration of production environment data for DBMS and non-DBMS applications at alternate processing site (hot-site), assuming the OPM network can service this activity. Restoration of NITC data center network • All data is asynchronously mirrored with minimal data loss • Recovery point objective (RPO) of less than or equal to 24 hours prior to disaster for mirrored production data	Reported on per event basis RTO means the maximum time within which the data center production environment will be restored after disaster declaration RPO means that customers will be able to restore their production data to a point less than or equal to 24 hours before the disaster occurred	• Severity 0: Entire facility is impacted and offline • The Disaster Recovery site will support up to 100% collective capacity of the production environment • DR does not include immediate support for agency development environments • NITC is responsible for establishing the current data center network environment, agencies need to restore portions of network they are responsible for
48 Hour Restoration	Severity 1 Response	• Immediate response • Production Environment: RTO of 48 hours for data center restoration when system problems occur that do not require to move to hot-site • RPO of 24 hours prior to disaster for restored production data	Reported on per event basis	• Severity 1: One or more systems or agencies impacted • Restoration can take place at current NITC location with some reallocation of existing resources

SQT	SQT Definition	SQT Metric	Measurement & Reporting	Comment/Assumption
DR Testing	NITC and Customer DR plans	• NITC will test disaster recovery plans at least annually • Customer agencies will test their internal disaster recovery procedures and plans during these test windows	NITC and customers will complete an analysis of DR testing results after each session to determine if changes and improvements are needed	• Testing will be conducted at the designated alternate processing site (currently located in St. Louis, Missouri)

7.2 Customer Disaster Recovery Responsibilities

Customer will participate in disaster recovery exercises for their mission critical applications and systems and will assist NITC in the evaluation of the DR testing results to determine where processes and procedures can be improved.

- Customer will identify and document the critical applications to be restored at the DR location, the order of recovery, and the time of recovery for each of these applications.
- Customer will arrange for telecommunications and network services at the DR location for the networks that they are currently responsible for (e.g., SNA banking network, connections to National Finance Center, USDA Wide Area Network).
- Customer is responsible for restoring to the correct version of a production application database once the DBMS production environment is in place at the DR site.
- Customer will use current system utilities, such as ABARS and RMM, for agency disaster recovery processes and backing up production data if applicable.

8 Data Center Facility

Reference Appendix L – NITC General Services, for details about NITC Facilities, Contract Management, and Service Management processes.

8.1 Server availability 24 hours a day, 7 days a week

Assure the shared environment will be available 24 hours per day, 365 days per year, except for scheduled downtimes. Scheduled downtime notifications will be made through Customer Memos and regular Customer Meetings. NITC will work with the customer to provide, monitor and control ADP resources and ensure system and network availability and efficient system performance.

The normal weekly maintenance schedule for the USDA shared environments are as follows:

Saturday 2400 CT through Sunday 0600 CT	**Customer Disaster Recovery Backups**
Sunday 1600 CT through Monday 0500 CT	**IPLs, System Maintenance**

Maintenance windows are scheduled but not always used or all the scheduled time utilized.

Non-USDA shared customers maintenance windows are mutually agreed upon by NITC and the customer.

Extended hours of service or changes to this schedule to accommodate program delivery requirements are coordinated in advance to assure adequate staffing.

8.2 USDA WAN connectivity

Maintain and operate the telecommunications infrastructure for connectivity to the Internet via the USDA backbone. 100 Megabit per second access to the server(s) will be provided via a TCP/IP network. Coordinate with the customer for any telecommunications infrastructure changes that would affect the operations of the project platform.

Telecommunications activities include:

- Plan and design telecommunications infrastructure
- Install/upgrade cable plants and wiring for all environments
- Troubleshoot and maintain telecommunications infrastructure
- Monitor and control telecommunications capacity

Table 8: Telecommunication

Activity	Tasks/Description
Plan and design telecommunications infrastructure	• Determine network requirements • Interface with customers telecommunications specialist, vendors, integrator • Establish roles and responsibilities (look at MOU) • Determine/coordinate/design network/IP address scheme and design • Determine network (IP) addresses and scheme • Establish levels of service • Coordinate with customer telecommunication specialists • Draw schematic diagrams
Install/upgrade cable plants and wiring for all environments	• Install servers, switches, routers, circuit, and wiring • Assess local exchange carriers equipment (how to tap in phone company wires) • Build new/host on existing network • Establish connectivity to NITC network infrastructure • Coordinate with security

Activity	Tasks/Description
Troubleshoot and maintain telecommunications infrastructure	• Create/receive problem record • Clarify problem • Diagnose network failures • Determine solution/coordinate with other telecommunications carriers and customers • Get approval for resolution • Resolve/schedule telecommunication issue • Determine outage/change- generate announcement • Escalate to customers/carriers • Monitor maintenance contracts requests/response time • Create maintenance program requirements
Monitor and control telecommunications capacity	• Track ports • Track availability • Forecast connectivity requirements (router, ports, switches) • Monitor IP addresses (masking/ segmentation) • Monitor utilization • Retire/sunset telecommunications equipment

8.3 Internet Intrusion Detection/Vulnerability Assessment

The NITC will provide constant network intrusion detection of unauthorized access to systems. Vulnerabilities in systems will be detected by scanning servers with Internet Scanner Software (ISS) on a monthly basis.

8.4 NITC Service Desk

The NITC Service Desk will accept calls from the customer first-level Point of Contact (POC) Contact List. The NITC Service Desk will document the request and assign a technical point of contact. If necessary, the individual from NITC's Service Desk will contact an on-call NITC technical specialist. NITC technical specialist will initiate calls to hardware and/or software vendors for support, track problems using the NITC problem and change management process, and coordinate with any involved parties.

9 Notification of anticipated downtime

NITC will provide a minimum of a 24-hour notice for any anticipated, but unscheduled downtime (e.g. if NITC must replace a piece of equipment that is giving a warning sign of failing) to the customer Point of Contact (POC). These downtimes generally will not exceed two hours and will be for the purpose of performing infrastructure, hardware, system software, or application software maintenance, or to perform data backups. All scheduled downtimes will be negotiated with the customer and will be planned to avoid downtime affecting peak usage time periods.

10 Notification of system failure

NITC will notify the appropriate customer POC (See Appendix A for Contact List) of failure or anticipated system failure, initiate procedures required to resume normal operations, and keep the customer POC apprised of progress towards resuming normal operations. Response to a trouble report will be initiated immediately during normal business hours, and within two hours outside of normal business hours.

10.1 System outage logs

NITC will maintain a log of all NITC system and network outages.

11 Billing

The NITC will bill the customer on a monthly basis in arrears as services are provided. After obtaining a user id (the procedure is described at the link below), customers may access the NITC internet based Billing System for usage data and charges and monthly invoice information at https://billing.nitc.usda.gov.

NATIONAL INFORMATION
TECHNOLOGY CENTER

Service Catalog

Version 4.2

USDA

Table of Contents

Why NITC

Why NITC 1

Why NITC Cloud Services....2

Service Desk 3

System and Network Control Center....4

Infrastructure as a Service

SAN / NAS Storage 5

Backup / Archive Storage....6

Network 7

Facility 8

Platform as a Service

Server....9

Mainframe 10

Web Server....11

Web Application Server....12

Web Portal....13

Database 14

Web Content Management 15

Document Management....16

Web Search....17

Web Accelerator (Akamai) 18

CloudVault 19

Virtual Application Desktop 20

Professional Services

Application Integration....21

Database Management....22

Project Management 23

Disaster Recovery....24

Planning and Integration 25

Other Hosting Services

Managed Hosting 26

Security Services

Information Systems and Network Security 27

Security Governance....28

Business Services

Business Management....29

Table of Contents

Procurement 30

Service Rates .... available upon request

Sample Service Agreement .... available upon request

Inheritable Controls Matrix .... available upon request

NATIONAL INFORMATION TECHNOLOGY CENTER

U.S. Department of Agriculture
Office of the Chief Information Officer

Data Center Services

The NITC Enterprise Solutions are developed utilizing government and industry standards and best practices. Our Level IV data center facilities utilize state-of-the-art, enterprise class infrastructure technologies to deliver optimal yet cost-effective solutions. NITC has a diverse and dedicated staff of Information Technology professionals who are proficient in systems architecture and integration, infrastructure management and operation, and disaster recovery. They work with customers to deliver secure and highly available solutions. The NITC secure IT infrastructure consists of virtualized mainframe and midrange platforms as well as virtualized network and storage infrastructure. The systems and applications managed by NITC are national in scope, mission critical, and essential for the operations of the United States government.

- **Infrastructure as a Service (IaaS):** The NITC Infrastructure as a Service provides a virtual machine infrastructure which allows customers the option to maintain control of their operating and general support systems at the system level. IaaS is provided for customers to maintain control of their hosting platform while allowing NITC to control the infrastructure on which it resides. NITC also offers three tiers of IaaS storage that are available to customers on demand.

- **Platform as a Service (PaaS):** The NITC Platform as a Service builds on the IaaS to provide customers with robust hardware platforms that are virtualized for optimal cost efficiency and flexibility. The underlying hardware is coupled with NITC Network and NITC Storage services to provide a fully managed operating platform up to and including one of the supported operating systems. In addition to the supported operating systems, NITC currently also offers various PaaS services including database, web portal, web server etc. The PaaS services include software license management and essential professional services for the products included in the service.

- **Managed Hosting:** For extremely large or unique applications that require dedicated hardware, NITC will manage customer provided servers up through the operating system (OS) in a secure operating environment including systems installation, engineering, administration, and support.

- **Professional Services:** NITC can provide the professional services required for integrating and administering enterprise-class business applications and databases, project management, and planning for technology advancements and disaster recovery.

Why NITC?

Experience

NITC has provided services as a federated data center since 1973 and has performed data center migrations since the 1980s. NITC cross-services 14 federal departments/bureaus.

Innovation

The NITC-managed Enterprise Data Center is a federally owned Cloud services provider; offering agencies enterprise class infrastructure built from the ground up with market leading technologies. NITC continues to innovate with the introduction of new Cloud services and utilize “green” industry best practices as much as possible to improve energy efficiency and reduce greenhouse gas emissions.

Customer Service

NITC offers 24x7 monitoring and expert technical support to ensure customers can focus on their core business without worrying about IT infrastructure.

CONTACT US

NITCServiceDesk@ocio.usda.gov
888-USE-NITC or 816-926-6660

NATIONAL INFORMATION TECHNOLOGY CENTER

U.S. Department of Agriculture
Office of the Chief Information Officer

NITC Cloud Services

NITC offers a broad range of Cloud services using virtualized, multi-tenant operating environments to offer several Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) services. NITC Cloud services offers:

- Rapid elasticity
- Scalable, pay-as-you-go pricing
- Monthly billing and predictable cost
- Periodic hardware refresh
- 99.99% availability
- Independent audits for OIG, A-123 and inheritable controls

Infrastructure as a Service (IaaS): The NITC Infrastructure as a Service provides a virtual machine infrastructure which allows customers the option to maintain control of their operating and general support systems at the system level. Network, Facility, Security, and Operational Support Services are included with all IaaS offerings.

Server – Coming Soon
SAN/NAS Storage - Tier 1, Tier 2, Tier 3, Replication
Backup/Archive Storage - Onsite, Offsite, Replication

Platform as a Service (PaaS): NITC PaaS offerings build upon IaaS offerings enables customers to select from secure, standardized Operating System images that are configured to meet actual processing requirement. Each PaaS offering is fully managed and maintained by NITC. In addition to the supported operating systems, NITC also provides PaaS offerings that include respective software licensing. By utilizing cost-effective platform solutions that are configured and licensed to meet actual application processing requirements, customers need only focus on the development and deployment of their business applications.

Server - Linux^{TM}, Windows^{TM}, Solaris^{TM}, AIX^{TM}
Mainframe - zOS^{TM}
Web Server - LAP, LAMP
Web Application & Web Portal Server - WebSphere^{TM}
Database - MySQL^{TM}, SQL Server^{TM}, Oracle^{TM}
Web Content & Document Management – Oracle UCM^{TM}
Web Search - Google^{TM}
Web Accelerator - Akamai^{TM}
Cloudvault - ownCloud
Virtual Application Desktop - Citrix^{TM}

Why NITC Cloud Services?

Rapid Provisioning

The NITC Cloud services offer virtualized instances of software, servers and storage that can be deployed for the customers within a very short period of time. In addition, virtualized environment supports rapid elasticity.

Predictable Cost Model

NITC Cloud service helps customers eliminate capital expenditure and improve operating efficiencies by using a multitenant hosting environment. Various standard and premium options and templates are offered to meet unique customer demand.

Customer Service

NITC offers dedicated account teams and 24x7 monitoring and expert technical support to ensure customers can focus on their core business without worrying about IT infrastructure.

CONTACT US

NITCServiceDesk@ocio.usda.gov
888-USE-NITC or 816-926-6660

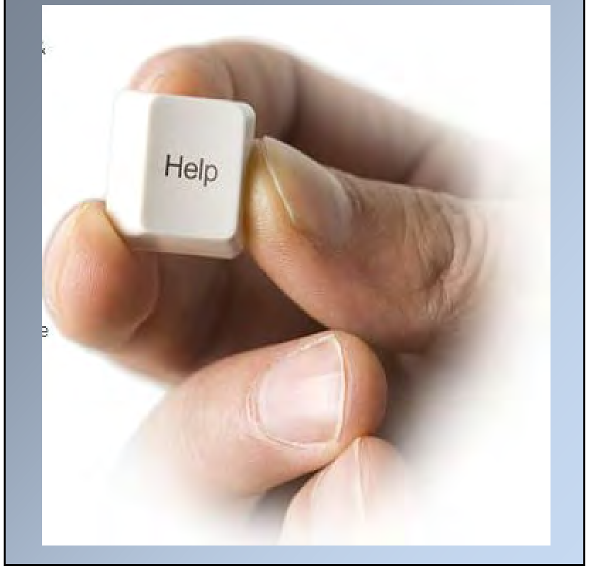
Service Desk

The NITC Service Desk is your single Point of Contact (POC) for managing incidents to resolution. The Service Desk facilitates the restoration of normal operational service to minimize business impact to the customer. The Service Desk is available 24 hours a day, 7 days a week, and utilizes Information Technology Service Management (ITSM) best practices to record, route, and manage the timely response to all service requests.

The NITC Service Desk supports customers daily with:

- Incident management
- Problem management
- Information requests
- Service requests
- Password resets
- Account permissions
- Connectivity issues
- Remote access
- Lost equipment notification

The NITC Service Desk plays an integral part in all NITC services.



When contacting the Service Desk for assistance:

- Be prepared to provide required information
  - Contact information
  - Relevant agency and system information
  - Information related to request
- Provide appropriate authorization for service requests
- Utilize optional email template

The NITC ITIL-based ITSM practices provide:

- Configuration Management Database (CMDB)
- Asset Management
- Configuration Management
- Release Management
- Change Management
- Incident Management
- Problem Management

Contact the NITC Service Desk at:

NITCServiceDesk@ocio.usda.gov
888-USE-NITC or 816-926-6660

System and Network Control Center

The NITC System and Network Control Center (SNCC) monitors the performance and availability of NITC managed systems and networks 24 hours a day, 7 days a week.

The NITC SNCC performs:

- System and network monitoring
- 2nd Tier Systems Administration support
  - Mainframe Initial Program Loads (IPLs)
  - System Reboots
  - Hardware Resets
  - Hardware Support
  - Software Support
- Production control functions
- Facility monitoring and management
  - Power and Environmental Equipment Support and Incident Resolution
  - Data Center Security and Access Control
- Tape management
  - Physical tape handling
  - Offsite tape rotation and retrieval
  - Coordination and deployment of media for disaster recovery
- Data component disposal
- 2nd Tier Incident and Problem Management support
- Certification of hardware/software changes

The NITC System and Network Control Center performs 24 x 7 monitoring and operations services.

When contacting the SNCC:

- Be prepared to provide required information
  - Contact information
  - Relevant agency and system information
  - Information related to request
- Provide appropriate authorization for service requests
- Utilize optional email template

Contact the SNCC via the NITC Service Desk at:

NITCServiceDesk@ocio.usda.gov
888-USE-NITC or 816-926-6660

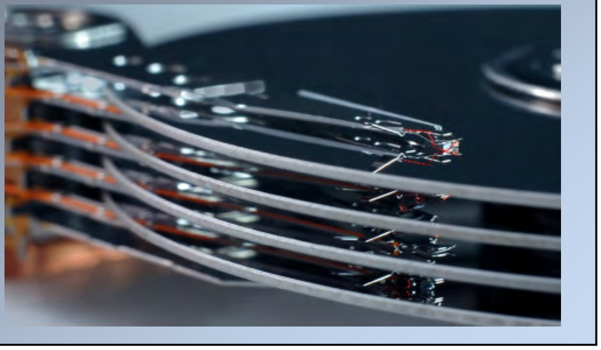
Infrastructure as a Service

National Information Technology Center

Service Desk: 888-USE-NITC

SAN / NAS Storage

NITC can provide a virtualized and highly-available disk storage infrastructure.



Service Description

The NITC Storage Area Network (SAN) / Network Attached Storage (NAS) service provides a robust disk storage infrastructure for Collocation, Managed Hosting, and Cloud Service customers. NITC exploits storage virtualization technologies, strict standards, and economies of scale to enable rapid delivery of cost-effective, fully-managed disk storage cost/performance options.

What is Included

- Enterprise-class virtualized disk storage controllers
    - High scalability
    - High performance
    - High availability
    - Robust data replication and migration features
        - Local disk cloning
        - Remote replication for disaster recovery
            - Primary Disk – Continuous
            - Backup Disk – Manual or Scripted
    - Three virtualized disk storage options
- Redundant SAN architecture
    - Dual-fabric architecture
    - Enterprise-class directors and switches
- Highly-available NAS infrastructure
    - Utilizes same virtualized disk architecture
    - Supports both NFS and CIFS file sharing
    - Robust data snapshot/replication technology
- Security of mission-critical data provided through management of access rights
- Periodic technology refresh
- Fully secured data access and inheritable controls
- Proper disposal of failed data components
- Disaster recovery support for replicated data
- Dynamic load balancing path management software
- Recommended Backup/Archive services are also available

Disk Storage Options

Option	Performance	SAN	NAS	Application Type
Tier 1	Best	x	x	Performance Sensitive
Tier 2	Better	x	x	Typical Applications
Tier 3	Good	x	x	Backup and Archive

How We Charge

Charges are based on connectivity requirements and actual disk allocations by tier.

Price drivers:

- Number of SAN/NAS ports utilized
- Storage Allocation in Gigabytes
- Additional charges may apply for storage allocation associated with any local or remote replication

Service Level Metrics

Measure	Service Level Targets
Infrastructure Monitoring	24 x 7
Incident Response	24 x 7
Infrastructure Availability	99.999%*

*Target availability does not include any scheduled downtime and requires dual SAN/NAS connectivity to the storage infrastructure.

Cost Saving Tips

- Utilize disk storage tiers appropriately
- Utilize provided path management software or native Operating System capabilities
- Utilize NAS solutions for highly available file sharing
- Proactively inform NITC of disk storage requirements

Additional Information

- File system and database recovery procedures are typically required for Disaster Recovery

Backup / Archive Storage

We provide a robust combination of hardware and software technologies for data protection and archive requirements.

Service Description

The NITC Backup / Archive Storage service provides a robust combination of hardware and software technologies for Collocation, Managed Hosting, and Cloud Service customers' data protection and archive requirements. NITC exploits tape virtualization and automation technologies to enable the delivery of cost-effective, fully-managed data protection and data lifecycle storage solutions.

What is Included

- Fully managed data protection and archive solutions
- Both onsite and offsite data storage available
- Enterprise-class virtual tape technology
  - High scalability
  - High performance
  - Remote data replication features
- Automated real tape technology
  - High-capacity tape drives
  - Fully automated tape libraries
- Automated data protection software
  - Network and SAN client software
  - Optional database client software
- Automated Archive Management Software
  - Automated archiving from disk to tape
  - SAN/NAS disk storage required
- Fully secured data access and inheritable controls
- Proper disposal of failed data components
- Disaster recovery support

Standard Backup Schedule and Retention*

Backup Type	Frequency	Onsite Retention	Offsite Retention
Full	Weekly	60 days	60 days
Incremental	Daily	14 days	14 days

*Backup schedule and retention periods are customizable

How We Charge

Charges are based on actual backup/archive data stored.

Price drivers:

- Total amount of data protected
- Change rate of data protected
- Required backup schedule
- Type of archive storage required
- Data retention periods

Service Level Metrics

Measure	Service Level Targets
Infrastructure Monitoring	24 x 7
Incident Response	24 x 7
Infrastructure Availability	99%*

*The NITC Backup/Archive solutions are designed to balance availability and control costs.

Cost Saving Tips

- Follow information lifecycle management best practices
  - Purge unused data
  - Retain only required data

Additional Information

- Customers are responsible for communicating any special backup schedule or retention requirements
- Customer provided equipment utilizing NITC Backup Services must provide additional network connectivity to the EDC Backup Network

Network

We provide robust Local Area Network connectivity and access to the USDA Wide Area Network and the Internet.

Service Description

The NITC Network Services include Local Area Network (LAN) connectivity for hosted systems and applications as well as connectivity to the USDA Wide Area Network (WAN) and the Internet.

What is Included

- Fully managed LAN infrastructure in each NITC Enterprise Data Center (EDC)
- Connectivity to the USDA Universal Telecommunications Network (UTN) WAN and Internet
- Network engineering and design consultation
- Network utilization monitoring and capacity planning
- Network load balancing and high availability solutions
- Fully integrated Network Security services
- Network cabling as required by NITC EDC standards

How We Charge

The cost of this service is included with other hosting services that rely on this service.

Hosting services that include Network Services:

- Platform as a Service
- Infrastructure as a Service
- Managed Hosting services

Service Level Metrics

Measure	Service Level Targets
System Monitoring	24 x 7
Incident Response	24 x 7
System Availability	≥99.99% excluding planned downtime*

* - NITC reserves the option to schedule its routine infrastructure maintenance activities on Sundays between 1800 to 2400 hours Central Time.

NOTE: NITC utilizes the USDA Universal Telecommunication Network (UTN) for Wide Area Network services. The USDA is contractually guaranteed to be 99.9% available but has historically delivered ≥99.99% availability.

Cost Saving Tips

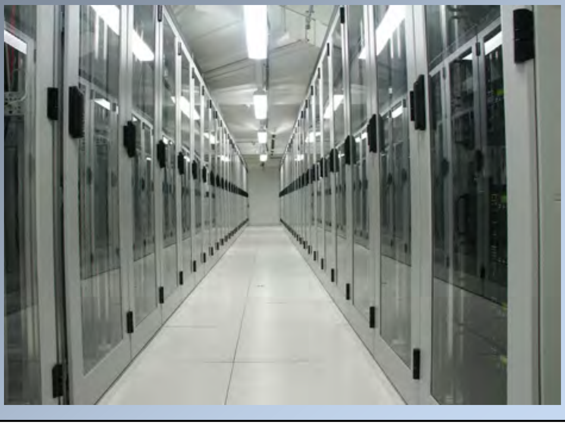
- Utilize NITC Network Services instead of hosting a private networking solution
- Provide at least 180 days' notice for growth or retraction of processing requirements
- Communicate projected networking requirements on a quarterly basis
- Limit internet usage to business related activities

Additional Information

- Customer provided equipment utilizing NITC Network Services must provide dual network connectivity to the EDC Highly-Available Network
- If optional Backup/Archive services are utilized, network connectivity to the EDC Backup network is also required

Facility (Enterprise Data Center)

We provide a secure, undisturbed system environment and data center infrastructure for hosting customer servers.



Service Description

NITC Facility Services provides an optimal Enterprise Data Center (EDC) operating environment for production customer application hosting. All NITC-managed EDCs adhere to USDA EDC standards and include key fault-tolerant characteristics equivalent to *Uptime Institute* Tier standards.

What is Included

Production Enterprise Data Centers

- **Kansas City, Missouri (Production)**
  Tier IV - Fault Tolerant Site Infrastructure
  A Fault Tolerant data center has multiple, independent, physically isolated systems that have redundant capacity components and multiple, independent, diverse, active distribution paths simultaneously serving the computer equipment.

- **Saint Louis, Missouri (Disaster Recovery)**
  Tier III - Concurrently Maintainable Site Infrastructure
  A concurrently maintainable data center with redundant capacity components and multiple, independent distribution paths serving the computer equipment.

Development, Test, and Disaster Recovery Center

- **Beltsville, Maryland**
  Tier 1 – Basic Site Infrastructure
  A basic data center with non-redundant capacity components and a single, non-redundant distribution path serving the computer equipment.

How We Charge

The cost of this service is included with other hosting services that rely on this service.

Hosting services that include Facility Services:

- Platform as a Service
- Infrastructure as a Service
- Managed Hosting services

Service Level Metrics

Measure	Service Level Targets
System Monitoring	24 x 7
Incident Response	24 x 7
Facility Availability	Beltsville (Tier 1) - 99.671%* Saint Louis (Tier III) - 99.982%* Kansas City (Tier IV) - 99.995%*

* - NITC reserves the right to schedule occasional infrastructure downtime and maintenance activities to accommodate growth and ensure optimal availability.

Cost Saving Tips

- Utilize NITC Enterprise Data Centers to obtain optimal business application availability
  - Kansas City for Production applications
  - St. Louis for Disaster Recovery

Additional Information

- Escorted access to the data center for authorized customer personnel can be scheduled to perform necessary operational tasks
- Certified DOJ Level IV Secure Facility
- USDA DM 3510-01 Physical Security Standards for Information Technology Compliant
- Security measures include:
  - Guard stations
  - Parking lot and exterior building surveillance
  - Computer room entry and egress surveillance
  - Computer room entry and egress secured with buffer zone and biometric access control

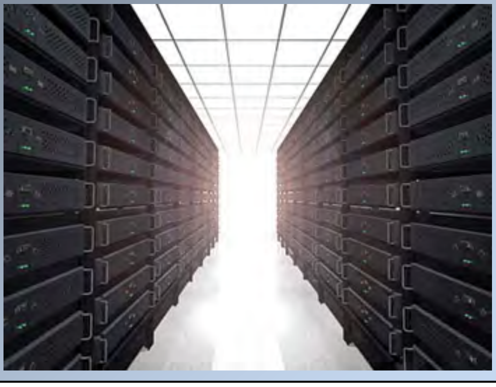
Platform as a Service

National Information Technology Center

Service Desk: 888-USE-NITC

Server

We provide standard virtualized operating platforms to securely host customer applications.



Service Description

The NITC Platform as a Service (PaaS) Server offering provides standard virtualized operating platforms to securely host customer applications. NITC utilizes advanced server virtualization technologies, strict standards, and economies of scale to enable rapid delivery of cost-effective, fully-managed operating platforms with expanded inheritable security controls**.**

What is Included

- Fully managed operating platform infrastructure
  - State-of-the-art server hardware
  - Standardized operating systems
  - SAN/NAS disk storage as required
  - Backup/Archive services as required
  - Highly available Network services
  - Redundant server hardware
  - Periodic technology refresh
- Full platform administration services
  - Virtual server configuration
  - Virtual OS installation
  - Virtual OS upgrades and patching
  - Security hardening per NIST standards
  - Application software installation
  - User management and audit log review
  - Virus protection and vulnerability mitigation
  - Disaster recovery support
  - Incident and problem resolution
- Systems engineering based on application requirements
- Related inheritable management controls
- Optional Virtual Desktop Platform as a Service
- Optional Professional Services such as
  - Database Management
  - Application Integration

Platform Options

Platform	Windows	Linux	AIX	Solaris
x86	X	X		
pSeries			X	
Sparc				X

How We Charge

Hosting charges are based on the number of virtual servers provided and actual allocated resources.

Price drivers:

- Number and type of virtual servers
- Amount of actual CPU and memory required
- Amount of actual Backup/Archive data retained
- Amount of actual SAN/NAS disk storage required
- Any RSA token requirements for Remote Access
- Additional charges may apply for optional Professional Services

Service Level Metrics

Measure	Service Level Targets
System Monitoring	24 x 7
Incident Response	24 x7
System Availability	99.99% excluding planned downtime*

* NITC reserves the option to schedule routine infrastructure maintenance activities on Sundays from 1800 to 2400 hours Central Time.

NOTE: NITC utilizes the USDA Universal Telecommunication Network (UTN) for Wide Area Network services. The UTN is contractually guaranteed to be 99.9% available but has historically delivered 99.997% availability.

Cost Saving Tips

- Be prepared to provide key hosting requirements to expedite the planning process

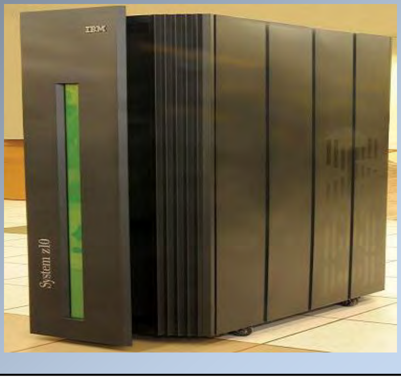
Additional Information

- Customers must allow NITC to maintain/update the Operating System to ensure vendor supportability
- Transitional IaaS is also available for application development and as a temporary solution to support Enterprise Data Center Consolidation

Platform as a Service

Mainframe

The NITC Mainframe Platform as a Service offering provides a fully managed platform for applications.



Service Description

The NITC Mainframe Platform as a Service includes a fully managed operating platform for mainframe-based applications. This fully-managed service includes systems engineering services, software tools, storage services, technology refresh, and disaster recovery.

What is Included

- Fully managed NITC Network Services and infrastructure
- Fully managed zOS™ operational environment
- Third party software tools, utilities, and support
- System security administration and support
- Capacity planning and performance tuning
- 24x7 system and network monitoring and support
- Fully managed disk and tape storage services
- Fully managed Disaster Recovery of the operating platform
- Application data recovery support
- Customer certification testing support
- Job scheduling and related monitoring
- Standard database administration activities
- Systems engineering and consulting services
  - Install, configure, customize, and maintain the Operating System and system utilities
  - Research, coordinate, and apply OS maintenance
  - Management, analysis, and review of OS system audit logging
  - Troubleshoot and resolve OS-related problems
  - Disk and Tape storage administration
  - Perform system tuning within the limits of NITC configuration standards
- Related inheritable management controls

How We Charge

Hosting charges are based on actual usage measurements.

Price drivers:

- Prime time and non-prime time CPU usage
- High, Normal, Medium, or Deferred Priority
- Amount of disk storage utilized
- Amount of tape storage utilized
- Additional charges may apply for
  - Specialized software
  - Database administration
  - Application support

Service Level Metrics

Measure	Service Level Targets
System Monitoring	24 x 7
Incident Response	24 x 7
System Availability	99.9% excluding planned downtime*

* - NITC reserves the option to schedule routine infrastructure maintenance activities on Sundays between 1800 to 2400 hours Central Time.

NOTE: NITC utilizes the USDA Universal Telecommunication Network (UTN) for Wide Area Network services. The UTN is contractually guaranteed to be 99.9% available but has historically delivered 99.997% availability.

Cost Saving Tips

- Adhere to the scheduled maintenance window
- Provide at least 180 days' notice for growth or retraction of processing requirements
- Communicate project processing requirements on a quarterly basis
- Participate in scheduled disaster recovery testing
- Archive data only when necessary
- Delete any unnecessary data
- Utilize standard tools and applications

Platform as a Service

Web Server

We provide a full service Web Server solution for static web applications.

Service Description

NITC provides an enterprise-class web server solution that meets agency requirements for light-weight web applications that require very little dynamic data. This offering includes simple scripting capable of supporting light-weight database updates and data retrieval.

What is Included

- Single Midrange Platform as a Service virtual server
  - Red Hat Enterprise Linux
  - Apache Web Server
  - PHP and Perl scripting modules
  - MySQL Database as required
- Key NITC Technical Services to install, patch, and upgrade software components
- System-level Database Administration services for MySQL component when required
- Additional virtual CPU, memory, and storage resources when required
- Optional Fault Tolerant and Disaster Recovery capabilities
- Optional Planning and Integration services
- Optional Application Integration services

Configuration Options

- LAP (Linux, Apache, and PHP)
- LAMP (Linux, Apache, MySQL, and PHP)

How We Charge

Hosting charges are based on the number of virtual servers provided and actual virtual resources allocated.

Price drivers:

- Number of LAP or LAMP base configurations required
  - Additional CPU, Memory, and/or Storage
  - Optional Fault Tolerance
- Optional Disaster Recovery
- Actual amount of optional Professional Services

Service Level Metrics

Measure	Service Level Targets
System Monitoring	24 x 7
Incident Response	24 x 7
System Availability	99.99% excluding planned downtime*
Website Metrics	Weekly log delivery

* - NITC reserves the option to schedule routine infrastructure maintenance activities on Sundays between 1800 to 2400 hours Central Time.

NOTE: NITC utilizes the USDA Universal Telecommunication Network (UTN) for Wide Area Network services. The UTN is contractually guaranteed to be 99.9% available but has historically delivered 99.997% availability.

Cost Saving Tips

- Engage NITC early in the scoping phase of a new project to identify all business and technical requirements
- Forecast response time and load expectations
- Utilize other OCIO service offerings to minimize application integration efforts and reduce costs through economies of scale

Web Application Server

We provide a full service Web Application Server environment for application hosting.

Service Description

NITC provides an enterprise-class web application server environment for robust, fault-tolerant web application hosting based on Java 2 Platform Enterprise Edition (J2EE) that includes:

JDK, EJB, Servlet, JSP, JMS, JDBC, JAX-RPC, SAAJ, Web Services for J2EE, JAXR, Java Authorization Contract for Containers, J2EE Management, J2EE Deployment, and J2EE Connectors

What is Included

- Single Midrange Platform as a Service (PaaS) virtual server
- WebSphere^{TM} Application Server software licensing and maintenance
- Key NITC Professional Services to install, patch, and upgrade software components
- System-level Database Administration services for database component of web application server
- Additional virtual CPU, memory, and storage resources as required
- Optional Fault Tolerant and Disaster Recovery capabilities
- Optional Planning and Integration services
- Optional Application Integration services

How We Charge

Hosting charges are based on actual number of virtual servers and resources utilized.

Price drivers:

- Number of Web Application Servers required
- Additional virtual server resources required (CPU, Memory, and Storage)
- Optional Fault Tolerance requirements
- Optional Disaster Recovery requirements
- Actual amount of optional Professional Services

Service Level Metrics

Measure	Service Level Targets
System Monitoring	24 x 7
Incident Response	24 x 7
System Availability	99.99% excluding planned downtime*
Website Metrics	Weekly log delivery

* - NITC reserves the option to schedule routine infrastructure maintenance activities on Sundays between 1800 to 2400 hours Central Time.

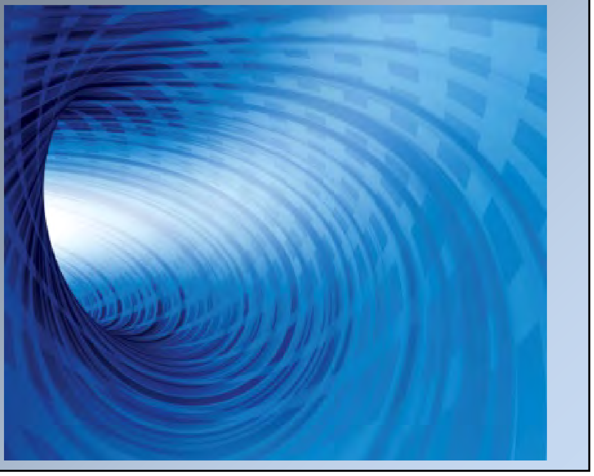
NOTE: NITC utilizes the USDA Universal Telecommunication Network (UTN) for Wide Area Network services. The UTN is contractually guaranteed to be 99.9% available but has historically delivered 99.997% availability.

Cost Saving Tips

- Engage NITC early in the scoping phase of a new project to identify all business and technical requirements
- Forecast response time and load expectations
- Utilize other OCIO service offerings to minimize application integration efforts and reduce costs through economies of scale

Web Portal

NITC provides a full service Web Portal solution for integrated web applications and content.



Service Description

NITC provides an enterprise-class portal solution for web application hosting that allows aggregation of applications and content for delivery as a single, role-based application.

.

What is Included

- Midrange Platform as a Service virtual servers
- WebSphere^{TM} Portal Server software licensing and maintenance
- Key NITC Technical Services to install, patch, and upgrade software components
- System-level Database Administration services for database component of web portal server
- Additional virtual CPU, memory, and storage resources when required
- Optional Fault Tolerant and Disaster Recovery capabilities
- Optional Planning and Integration services
- Optional Application Integration services

How We Charge

Hosting charges are based on actual number of virtual servers and resources utilized.

Price drivers:

- Number of Web Portal servers required
- Additional virtual server resources required (CPU, Memory, and/or Storage)
- Optional Fault Tolerance requirements
- Optional Disaster Recovery requirements
- Any additional Professional Services

Service Level Metrics

Measure	Service Level Targets
System Monitoring	24 x 7
Incident Response	24 x 7
System Availability	99.99% excluding planned downtime*
Website Metrics	Weekly log delivery

* - NITC reserves the option to schedule routine infrastructure maintenance activities on Sundays between 1800 to 2400 hours Central Time.

NOTE: NITC utilizes the USDA Universal Telecommunication Network (UTN) for Wide Area Network services. The UTN is contractually guaranteed to be 99.9% available but has historically delivered 99.997% availability.

Cost Saving Tips

- Engage NITC early in the scoping phase of a new project to identify all business and technical requirements
- Forecast response time and load expectations
- Utilize other OCIO service offerings to minimize application integration efforts and reduce costs through economies of scale

Platform as a Service

Database

NITC provides a fully managed Database platform solution for use as an integral part of an application hosting environment.

Service Description

The NITC Database Platform as a Service offering provides a fully managed platform solution for use as an integral part of an overall customer application hosting environment. The offering provides scalable database services that provide required performance, reliability, and functionality while also providing cost savings associated with the overall ease of management and the economies of scale associated with a common, standardized solution.

What is Included

Fully managed database server

- Fully managed virtual server
- Standardized storage configurations
  - Data Files
  - Transaction Logs
  - Database Backups
- Database software licensing and maintenance
- Database software installation and configuration
- Database operations, patching, and maintenance
- Operating System and Database Administration
  - Software installation and maintenance
  - System-level patching and support
- Full database and transaction log backups for Point-In-Time database recovery
- System and Database monitoring services

Database Software Options

- Microsoft™ SQL Server™
- Oracle™
- MySQL™

How We Charge

Hosting charges are based on the number of virtual servers provided and actual allocated resources.

Price drivers:

- Number of Database virtual servers required
  - Optional High Availability
  - Optional Disaster Recovery
- Amount of actual CPU and memory required
- Amount of data storage required in 10GB increments
- Additional charges for optional data retention periods
- Additional charges for optional Professional Services

Service Level Metrics

Measure	Service Level Targets
System Monitoring	24 x 7
Incident Response	24 x 7
System Availability	99.99% excluding planned downtime*
Notification Services	Available upon request

* - NITC reserves the option to schedule routine infrastructure maintenance activities on Sundays between 1800 to 2400 hours Central Time.

NOTE: NITC utilizes the USDA Universal Telecommunication Network (UTN) for Wide Area Network services. The UTN is contractually guaranteed to be 99.9% available but has historically delivered 99.997% availability.

Cost Saving Tips

- Engage NITC early in the scoping phase of a new project to identify all business and technical requirements
- Utilize other OCIO service offerings to minimize application integration efforts and reduce costs through economies of scale

Web Content Management

NITC provides a full service Web Content Management solution.

Service Description

The NITC Web Content Management solution enables all authorized users within an organization to create, capture, store, manage, publish, view, search, archive all types of documents, and provides the ability to support the entire content management lifecycle.

Contributors are granted the ability to publish content directly, without a web masters intervention, vastly increasing the speed of making information available on the web.

What is Included

- Midrange Platform as a Service virtual server resources
- Oracle™ Universal Content Management software licensing and maintenance
- Key NITC Technical Services to install, patch, and upgrade software components
- System-level Database Administration services for database component of web content management
- Additional virtual CPU, memory, and storage resources when required
- Optional Fault Tolerant and Disaster Recovery capabilities
- Optional Planning and Integration services
- Optional Application Integration services

How We Charge

Hosting charges are based on actual number of virtual servers and resources utilized.

Price drivers:

- Actual number of Web Content Management solutions required
- Additional virtual server resources required (CPU, Memory, and/or Storage)
- Optional Fault Tolerance requirements
- Optional Disaster Recovery requirements
- Any additional Professional Services

Service Level Metrics

Measure	Service Level Targets
System Monitoring	24 x 7
Incident Response	24 x 7
System Availability	99.99% excluding planned downtime*
Website Metrics	Weekly log delivery

* - NITC reserves the option to schedule routine infrastructure maintenance activities on Sundays between 1800 to 2400 hours Central Time.

NOTE: NITC utilizes the USDA Universal Telecommunication Network (UTN) for Wide Area Network services. The UTN is contractually guaranteed to be 99.9% available but has historically delivered 99.997% availability.

Cost Saving Tips

- Engage NITC early in the scoping phase of a new project to identify all business and technical requirements
- Forecast response time and load expectations
- Utilize other OCIO service offerings to minimize application integration efforts and reduce costs through economies of scale

Platform as a Service

National Information Technology Center

Service Desk: 888-USE-NITC

Document Management

NITC provides a full service Document Management solution.

Service Description

The NITC document management solution allows organizations to effectively and efficiently capture, secure, share and distribute digital and paper-based documents. The solution includes a workflow process to mirror the review of information and supports process automation for document creation, review, and revision.

What is Included

- Single Midrange Platform as a Service virtual server
- Oracle™ Universal Content Management software licensing and maintenance
- Key NITC Technical Services to install, patch, and upgrade software components
- System-level Database Administration services for database component of Document management
- Additional virtual CPU, memory, and storage resources when required
- Optional Fault Tolerant and Disaster Recovery capabilities
- Optional Planning and Integration services
- Optional Application Integration services

How We Charge

Hosting charges are based on actual number of virtual servers and resources utilized.

Price drivers:

- Number of Document Management solutions required
- Additional virtual server resources required (CPU, Memory, and/or Storage)
- Optional Fault Tolerance requirements
- Optional Disaster Recovery requirements
- Any additional Professional Services

Service Level Metrics

Measure	Service Level Targets
System Monitoring	24 x 7
Incident Response	24 x 7
System Availability	99.99% excluding planned downtime*
Website Metrics	Weekly log delivery

* - NITC reserves the option to schedule routine infrastructure maintenance activities on Sundays between 1800 to 2400 hours Central Time.

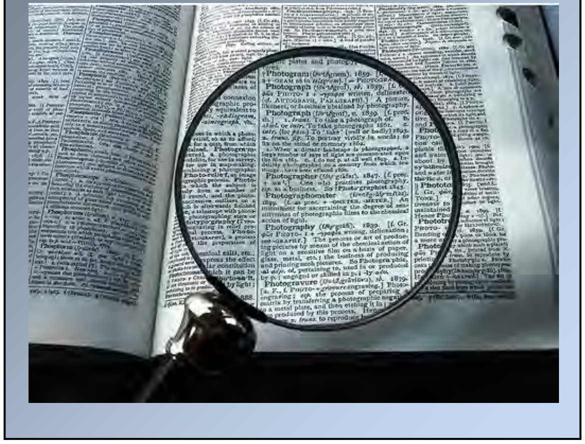
NOTE: NITC utilizes the USDA Universal Telecommunication Network (UTN) for Wide Area Network services. The UTN is contractually guaranteed to be 99.9% available but has historically delivered 99.997% availability.

Cost Saving Tips

- Engage NITC early in the scoping phase of a new project to identify all business and technical requirements
- Forecast response time and load expectations
- Utilize other OCIO service offerings to minimize application integration efforts and reduce costs through economies of scale

Web Search

NITC provides customizable enterprise search capabilities for web applications.



Service Description

The NITC Enterprise Search offering provides customizable, web search-engine functionality for web applications. The solution can be configured to search collections of web pages that are customized per application. These collections can include anything from the entire domain to a single web page. The search catalog offers services for public facing and protected sites using USDA's SSO (eAuthentication) system.

What is Included

- Best-in-class appliance-based search
- Cross-site, cross-agency, cross-department search capability
- Customizable search based on website logical design
- Customizable search result output
- File system, Web repository, Database, Feed, Connector, OneBox module-based crawl ability
- Secure site crawl-ability (eAuthentication)

How We Charge

Hosting charges are based on the following factors:

- Actual number of website URLs crawled
- Setup fee for highly customized integrations

Service Level Metrics

Measure	Service Level Targets
System Monitoring	24 x 7
Incident Response	24 x 7
System Availability	99.99% excluding planned downtime*
Website Metrics	Weekly log delivery

* - NITC reserves the option to schedule routine infrastructure maintenance activities on Sundays between 1800 to 2400 hours Central Time.

NOTE: NITC utilizes the USDA Universal Telecommunication Network (UTN) for Wide Area Network services. The UTN is contractually guaranteed to be 99.9% available but has historically delivered 99.997% availability.

Cost Saving Tips

- Engage NITC early in the scoping phase of a new project to identify all business and technical requirements
- Forecast response time and load expectations
- Utilize other OCIO service offerings to minimize application integration efforts and reduce costs through economies of scale

Web Accelerator (Akamai)

NITC can provide Web Accelerator service to further enhance web application performance and availability.

Service Description

NITC can provide 3rd party Akamai Web Accelerator service to further enhance web application performance and availability as well as deliver static websites. Front end redundancy and geographically dispersed nodes for last loop efficiency are included.

Built upon Akamai's EdgeAdvantage™ platform, Akamai's Dynamic Site Accelerator™ solution introduces intelligent content generation and comprehensive site delivery at the edge and provides E-businesses with the optimal solution for dynamic website availability, scalability and performance.

What is Included

- Akamai’s global Content Delivery Network (CDN)
- Basic and Encrypted (SSL) content acceleration
- Live and on-Demand streaming
- NetStorage for online storage
- Management Console to manage content
- Optional Akamai professional services support

How We Charge

Hosting charges are based on the following factors:

- Actual usage of licensed service based on bandwidth and storage consumption
- Actual number of optional Akamai professional service hours

Service Level Metrics

Measure	Service Level Targets
System Monitoring	24 x 7
Incident Response	24 x 7
System Availability	99.99% excluding planned downtime*
Website Metrics	Weekly log delivery

* - NITC reserves the option to schedule routine infrastructure maintenance activities on Sundays between 1800 to 2400 hours Central Time.

NOTE: NITC utilizes the USDA Universal Telecommunication Network (UTN) for Wide Area Network services. The UTN is contractually guaranteed to be 99.9% available but has historically delivered 99.997% availability.

Cost Saving Tips

- Engage NITC early in the scoping phase of a new project to identify all business and technical requirements
- Forecast response time and load expectations
- Utilize other OCIO service offerings to minimize application integration efforts and reduce costs through economies of scale

Platform as a Service

CloudVault

NITC can provide collaboration on the cloud through its cloud based storage service

Service Description

NITC can provide collaboration on the cloud through its secured cloud based storage service. This cloud based remote storage capability is accessible from the Internet through mobile device, browser, or thick client which will provide agencies/organizations the capability to have their own private cloud storage. Users of cloud storage can share content with other cloud storage users within that domain.

What is Included

- NITC PaaS and Storage Services
- Web based interface to securely upload and download files
- Version control
- Sharing of files with both registered and no-registered users
- Secure file sharing with password and expiration date
- Downloadable sync clients to sync from your desktop , laptop and mobile devices

How We Charge

Hosting charges are based on the following factors:

- Number of registered users within CloudVault
- Actual storage used within CloudVault

Service Level Metrics

Measure	Service Level Targets
System Monitoring	24 x 7
Incident Response	24 x 7
System Availability	99.99% excluding planned downtime*

* - NITC reserves the option to schedule routine infrastructure maintenance activities on Sundays between 1800 to 2400 hours Central Time.

NOTE: NITC utilizes the USDA Universal Telecommunication Network (UTN) for Wide Area Network services. The UTN is contractually guaranteed to be 99.9% available but has historically delivered 99.997% availability.

Cost Saving Tips

- Engage NITC early in the scoping phase of a new project to identify all business and technical requirements
- Forecast response time and load expectations
- Utilize other OCIO service offerings to minimize application integration efforts and reduce costs through economies of scale

Virtual Application Desktop (Citrix)

NITC can provide virtual desktop technology to enable remote Data Center hosting of workstation-centric business applications.

Service Description

The NITC Virtual Desktop service provides the technology necessary to enable the hosting of workstation-centric business applications remotely in the NITC Enterprise Data Center. Combined with other key enabling NITC cloud services, the Virtual Application Desktop service can provide a practically identical end user experience for workstation-centric applications while simplifying the management of desktop software installation and maintenance and providing a secure remote access solution.

What is Included

- Fully managed and maintained infrastructure
  - State-of-the-art server hardware & software
  - Period technology refresh
- Both shared and dedicated solutions available
- Citrix™XenApp™
  - Virtual presentation of specific applications
  - Most cost effective virtual desktop solution
- Citrix™XenDesktop™
  - Virtual presentation of complete desktop
  - Provides users with desktop functionality

How We Charge

Costs are based on actual application hosting requirements and virtual application integration services required.

Price drivers:

- Actual shared or dedicated hosting requirements
- Number of concurrent users of XenApp™ integrated applications
- Number of XenDesktop™ integrated desktops
- Virtual Application Desktop application integration services as required

Service Level Metrics

Measure	Service Level Targets
System Monitoring	24 x 7
Incident Response	24 x 7
System Availability	99.9% excluding planned downtime*

* - NITC reserves the option to schedule routine infrastructure maintenance activities on Sundays between 1800 to 2400 hours Central Time.

NOTE: NITC utilizes the USDA Universal Telecommunication Network (UTN) for Wide Area Network services. The UTN is contractually guaranteed to be 99.9% available but has historically delivered 99.997% availability.

Cost Saving Tips

- Utilize other OCIO service offerings to minimize application integration efforts and reduce costs through economies of scale

Application Integration

NITC can provide key integration and application administration services.

Service Description

NITC can provide the professional services required for integrating and administering enterprise-class business applications.

What is Included

- Application architecture planning
- Application integration expertise and consultation
- Application software installation, maintenance, and support
- Supported Applications Services include:
  - IBM HTTP Web server™
  - IBM WebSphere Application Server™
  - IBM WebSphere Portal™
  - Oracle/Stellent Content Management™
  - Google Enterprise Search™
  - IBM MQ Series™

How We Charge

Charges are based on actual numbers of professional services hours.

Price drivers:

- Scope and timeframe of integration project
- Required software licenses
- Additional charges may apply for
  - Platform as a Service
  - Infrastructure as a Service
  - Other Professional Services

Service Level Metrics

Measure	Service Level Targets
Incident Response	24 x 7

Cost Saving Tips

- Avoid greater costs associated with high priority service
- Engage project team early to document requirements
- Minimize changes during project delivery
- Avoid historical project cost estimation
- Ensure that all requirements are documented

Additional Information

- Customer acceptance of deliverables is required
- Administration and support for other application software is considered on a case-by-case basis

Database Management

NITC can provide Database administration and consulting services.

Service Description

NITC Database Management services can provide the necessary professional expertise to install, configure, operate, and maintain industry standard database software.

What is Included

- Database engineering and architecture design
- Database software installation and configuration
- Database operations, patching, and maintenance
- Initial database installation and integration
- Database backup and recovery
- Pre-production and testing support
- Management of privileged user accounts to manage tables, indexes, and other data structures
- Problem and incident management
- Performance tuning and troubleshooting

The full suite of standard offerings includes:

	Platform		
Database	Midrange	z/OS	z/Linux
DB2	x	x	x
Oracle™	x		x
SQLServer	x		
MySQL	x		

How We Charge

Charges are based on actual number of professional services hours.

Price drivers:

- Size and number of database instances
- Number and frequency of database refreshes
- Actual software licensing and maintenance
- Additional charges may apply for
  - Platform as a Service
  - Infrastructure as a Service
  - Other Professional Services

Service Level Metrics

Measure	Service Level Targets
Incident Response	24 x 7

Cost Saving Tips

- Utilize standard software platforms
- Establish archive and purge criteria to minimize storage requirements

Additional Information

- Support for non-standard Database requests will be evaluated on a case-by-case basis

Project Management

NITC can provide experienced project managers to ensure timely success of service delivery projects.

Service Description

Project managers work closely with customers, vendors, and NITC functional areas to coordinate efforts and provide necessary project management functions to ensure timely project success.

What is Included

- Development of Project Charter
- Development of project plan and schedule
- Coordination and scheduling of project activities across customer and NITC functional areas
- Consultation on operational and infrastructure requirements, standards and configurations
- Assistance with standard requests for service
- Facilitate project status meetings
- Timely project status reporting
- Address project issues with NITC functional areas and management
- Escalation of significant issues to customers and NITC executive management
- Manage project scope and deliverable requirements
- Document changes to project scope and schedule
- Facilitate and document project closeout
- Access to the Project Management Resource Center

How We Charge

Current pricing is based on time and materials. Customer will only be billed for actual hours worked.

Price drivers:

- Complexity and scope of the project
- Number of functional areas involved

Cost Saving Tips

- Avoid higher costs associated with high priority service
- Engage project team early to document requirements
- Minimize changes during project delivery
- Avoid historical project cost estimation
- Ensure that all requirements are documented

Additional Information

- Customer signoff of deliverables and releases is required
- Utilize other OCIO service offerings to minimize application integration efforts and reduce costs through economies of scale

Disaster Recovery

NITC can provide Disaster Recovery planning and coordination services.

Service Description

NITC can provide assistance to customers with their Disaster Recovery (DR) planning, coordination, and incident response based on the Customer’s Business Impact Analysis (BIA), Recover Point Objectives (RPO), Recovery Time Objectives (RTO), and overall recovery priority.

What is Included

- Facilitation, planning, and coordination with NITC and Customer technical staff and coordinators to:
  - Assist with customer application Business Impact Analysis
  - Co-develop customer application Disaster Recovery Plans and recovery procedures
  - Participate in table-top Disaster Recovery Exercises
  - Participate in functional Disaster Recovery Exercises
  - Assist with documenting customer Test, Training, and Exercise (TT&E) programs and After Action Reports

How We Charge

Charges are based on actual numbers of professional services hours.

Price drivers:

- Frequency and complexity of DR planning
- Frequency and complexity of DR testing

Service Level Metrics

Possible Disaster Recovery Options

Service / Option	RTO	RPO*
Database Replication	2 hours	2 hours
Disk Replication	4 hours	2 hours
Tape Replication	24 hours	24 hours
Offsite Tape Rotation	72 hours	72 hours

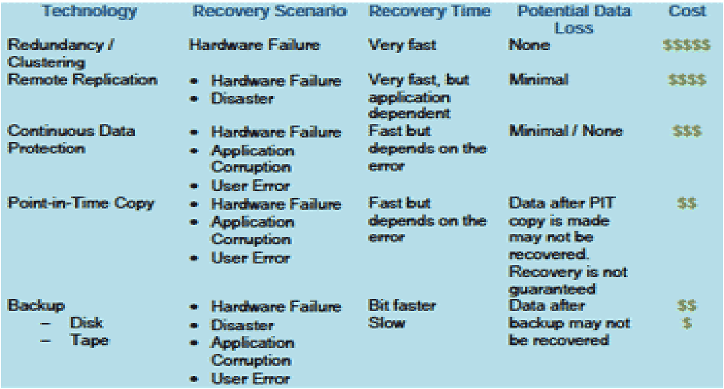
* - Actual RPO is dependent on critical component availability for the timely replication of data.

Cost Saving Tips

- Purge or archive unused data
- Perform a Business Impact Analysis to determine application RTO and RPO requirements
- Ensure the appropriate data protection solution is utilized to meet actual RTO and RPO requirements.

Additional Information

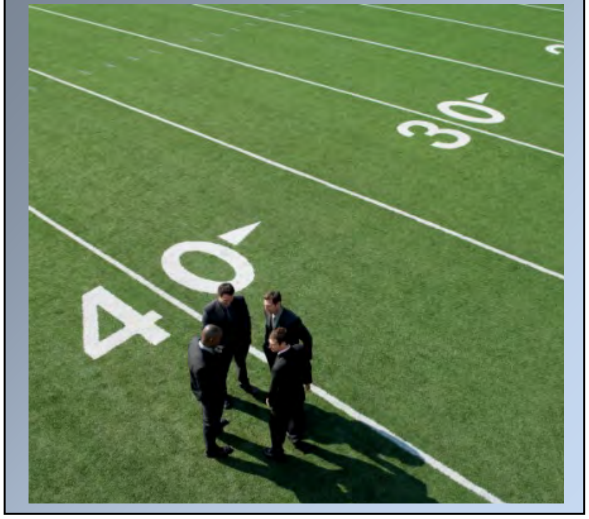
Typical Recovery Options and Relative Costs



Technology	Recovery Scenario	Recovery Time	Potential Data Loss	Cost
Redundancy / Clustering	Hardware Failure	Very fast	None	$$$$$
Remote Replication	• Hardware Failure • Disaster	Very fast, but application dependent	Minimal	$$$$
Continuous Data Protection	• Hardware Failure • Application Corruption • User Error	Fast but depends on the error	Minimal / None	$$$
Point-in-Time Copy	• Hardware Failure • Application Corruption • User Error	Fast but depends on the error	Data after PIT copy is made may not be recovered. Recovery is not guaranteed	$$
Backup – Disk – Tape	• Hardware Failure • Disaster • Application Corruption • User Error	Bit faster Slow	Data after backup may not be recovered	$$ $

Planning and Integration

NITC can provide the technical expertise to help design, plan, and integrate enterprise-class solutions.



Service Description

NITC can provide key professional services to assist customers in the design, planning, and integration of enterprise-class solutions. These key services help eliminate project risk and deliver robust technology solutions based on industry-best practices.

What is Included

- Insight into industry and department
  - Technology roadmaps
  - Strategic plans
  - Best Practices
  - Lessons learned
- Integration and project planning support
- Business requirements analysis
- Technical requirements identification
- Technical architecture solution design
- Project risk identification and prioritization
- Definition of Enterprise Data Center (EDC) standards
- Standard architecture governance
- Technical disaster recovery planning
- Capital investment analysis
- Technology and system integration cost estimation

How We Charge

Charges are based on actual number of professional services hours.

Price drivers:

- Scope and timeframe of technology project
- Additional charges may apply for
  - Platform as a Service
  - Infrastructure as a Service
  - Other Professional Services

Cost Saving Tips

- Avoid greater costs associated with high priority service
- Engage project team early to document requirements
- Minimize changes during project delivery
- Avoid historical project cost estimation
- Ensure that all requirements are documented

Additional Information

- Customer acceptance of deliverables is required
- Utilize other OCIO service offerings to minimize application integration efforts and reduce costs through economies of scale

Other Hosting Services

National Information Technology Center

Service Desk: 888-USE-NITC

Managed Hosting

We manage your servers up through the Operating System while providing a secure operating environment.

Service Description

NITC will manage customer-provided servers up through the Operating System (OS) in a secure operating environment including systems installation, engineering, administration, and support.

What is Included

- NITC enterprise class Facility services
- Availability and utilization monitoring
- Customer notification of related incidents
- Physical equipment installation assistance
- Cabling services per Enterprise Data Center standards
- Optional customer asset disposal
- Full Operating Systems administration services
  - Limited systems engineering
  - OS installation and customization
  - OS upgrades and patching
  - Security hardening per NIST standards
  - Application software installation assistance
  - User management and audit log review
  - Virus protection and vulnerability mitigation
  - Disaster recovery support
  - Incident and problem resolution
- Optional SAN/NAS disk storage services
- Backup/Archive services with customizable retention
- Network services
  - Local and Wide Area Networking
  - Network Security Services
- Related inheritable management controls
- Optional Professional Services such as:
  - Planning and Integration
  - Application Integration
  - Database Management
  - Project Management

Supported Operating Systems

	Server Platform		
Operating System	x86	Sparc	pSeries
VMWare ™	x		
Windows ™	x		
Redhat ™	x		
Solaris ™	x	x	
AIX ™			x

How We Charge

Hosting charges are based on the number of physical and virtual servers managed.

Price drivers:

- Amount of actual cabling and rack space required
- Amount of actual Backup/Archive data retained
- Additional charges may apply for
  - Optional SAN/NAS disk storage
  - Optional Professional Services

Service Level Metrics

Measure	Service Level Targets
System Monitoring	24 x 7
Incident Response	24 x 7
System Availability	Varies by customer environment

NOTE: NITC utilizes the USDA Universal Telecommunication Network (UTN) for Wide Area Network services. The UTN is contractually guaranteed to be 99.9% available but has historically delivered 99.997% availability.

Cost Saving Tips

- Utilize NITC Network services
- Utilize NITC SAN/NAS and Backup/Archive services
- Utilize server virtualization to reduce hosting costs

Additional Information

- Customers are required to adhere to NITC Enterprise Data Center power, racking and cabling standards.
- Customers are required to adhere to NITC Network vulnerability mitigation policy
- Customers must allow NITC to maintain/update the Operating System to ensure vendor supportability

Information Systems and Network Security

NITC provides key information and network security services to ensure a safe operating environment for business applications.

Service Description

NITC provides Information Systems and Network Security services that provide safe network access, security administration, monitoring and assessment to meet data security management requirements.

What is Included

NITC performs the following system security tasks for systems physically and/or logically located within the NITC Enterprise Network boundaries:

- Enterprise Network Firewall and Access Control List administration
- Enterprise Network Remote Access and Admission Controls administration
- Enterprise Network Intrusion Detection System (IDS) monitoring
- Enterprise Operating System (OS) vulnerability scanning and reporting to the Customer System Security Officer
- Enterprise compliance scanning to ensure the systems are maintained with proper baseline configuration standards and patch management
- Identity and Access Management administration which includes:
  - OS level security in the form of User ID/Password verification
  - Enforce strict security policies regarding system access
- Optional Application Scanning is available for an additional cost

How We Charge

With the exception of Application Scanning, the cost of this service is included when NITC Network Services are utilized.

Hosting services that include Network Security Services:

- Platform as a Service
- Infrastructure as a Service
- Managed Hosting services

Costs associated with optional Application Scanning services are based on software license fees and amount of actual professional services hours incurred

Service Level Metrics

Measure	Service Level Targets
System Monitoring	24 x 7
Incident Response	24 x 7

Cost Saving Tips

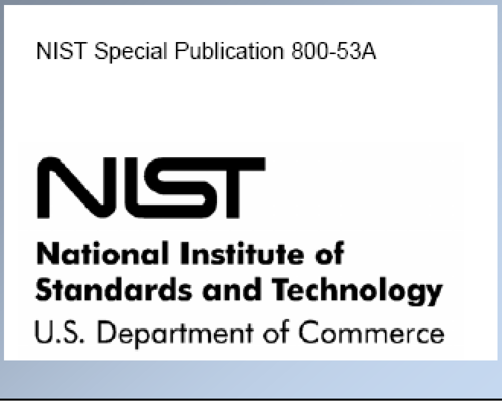
- Utilize NITC Network Services instead of hosting a private networking solution
- Provide at least 180 days’ notice for growth or retraction of processing requirements
- Communicate projected networking requirements on a quarterly basis
- Limit internet usage to business related activities

Additional Information

NITC also provides Security Governance Services that include limited control documentation, control inheritance, and audit support.

Security Governance

NITC can provide information and assurance that NITC services comply with mandatory security controls.



NIST Special Publication 800-53A

NIST

National Institute of Standards and Technology

U.S. Department of Commerce

Service Description

NITC provides information and assurance that NITC services comply with mandatory security controls.

What is Included

- FISMA compliance for NITC-provided services
- Standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets
- Supervision and oversight of NITC activity to ensure enforcement and monitor usage of information system access controls
- Security controls review to enable more consistent, comparable, and repeatable assessments
- Annual internal and 3rd party audits and assessments of security controls to determine overall control effectiveness
- Risk Management Framework for security categorization, security control selection and implementation, control assessment, information system authorization, and control monitoring
- More complete, reliable, and trustworthy information for organizational officials, to support security accreditation decisions, information sharing, and FISMA compliance

How We Charge

This critical value-added service is included with NITC Hosting Services.

Hosting services that include Security Governance:

- Platform as a Service
- Infrastructure as a Service
- Managed Hosting services

Service Level Metrics

Measure	Service Level Targets
Inquiry Response	8 x 5
Audit Results	Annual
Control Inheritance Matrix	Upon Request*
Control Descriptions	Upon Request*

* - Documentation provided is controlled and For Official Use Only (FOUO)

Cost Saving Tips

- Utilize a full complement of NITC services to obtain the most inheritable management controls

Relative Control Inheritance

NITC Service	NITC Network	NITC Storage	Inheritable Controls
Managed Hosting	No	No	✓ ✓ ✓ ✓
	Yes	No	✓ ✓ ✓ ✓ ✓
	Yes	Yes	✓ ✓ ✓ ✓ ✓ ✓
Infrastructure as a Service	Yes	Yes	✓ ✓ ✓ ✓ ✓ ✓ ✓
Platform as a Service	Yes	Yes	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓

Additional Information

A full matrix of inheritable management controls that identifies which controls are potentially inheritable as part of NITC's other hosting services is available upon request.

Business Management

NITC Account Managers help translate individual business needs into technical requirements and help customers find their way to optimal service delivery.

Service Description

Account Managers dramatically enhance the overall NITC customer experience by assisting with the translation of business application needs into technical hosting requirements and by providing an escalation point for customer services issues.

What is Included

- Ongoing customer relationship management
  - Develop an understanding of customer business functions
  - Identify customer business requirements
  - Assist with the definition of technical requirements
  - Represent NITC functional areas and the overall service delivery process
  - Provide an escalation point to customer service delivery issues
  - Ensure that key issues are escalated to NITC executive management
- Provide information about available NITC services and related costs
- Facilitate customer meetings regarding new projects with NITC functional areas
- Provide pricing estimates for new projects and changes to existing services
- Establish and maintain formal customer service agreements
  - Financial analysis to forecast usage and growth/retraction requirements
  - Monitor actual billing and make changes to agreements as necessary
- Monitor the overall Service Management lifecycle from establishment through retirement
- Provide information regarding planned changes to NITC services for strategic planning purposes
- Collect planned capacity and technical requirements and ensures information is included in NITC strategic planning and capacity forecasts

How We Charge

This key value-added service is included with other NITC services at no extra cost.

Cost Saving Tips

- Provide thorough business and technical requirements
- Utilize Planning and Integration Services to architect the hosting solution and identify all potential costs
- Utilize NITC Project Management Services to ensure timely project delivery
- Utilize Disaster Recovery Services to plan and coordinate DR testing
- Minimize changes during project delivery
- Avoid historical project cost estimation
- Keep Account Mangers informed of planning changes and capacity requirements

Procurement

Procurement Services enhance the NITC customer experience and provide additional savings through consolidation of buying power.

Service Description

NITC Procurement Services enhance the customer experience by providing centralized support for key contract negotiations. This value added service can optionally be utilized to acquire necessary equipment, software, and services to provide a total customer solution.

What is Included

- Acquisition consultation and assistance
- Cost Savings through economies of scale
- Acquisition support for funded procurements
  - Equipment
  - Software
  - Services
  - Maintenance
- Acquisition Life Cycle Management
  - Requirements Definition
  - Request for Proposal (RFP) development support
  - Technical and Business proposal evaluation
  - Contract Management
- Vendor management

How We Charge

A 5% service fee is applicable to new hardware and software procurements.

Ongoing Hardware and Software maintenance renewals that are part of combined enterprise contracts are free of charge.

Acquisition costs for hardware, software, and services are passed on to customers via reimbursable agreements.

Cost Saving Tips

- Utilize available Blanket Purchase Agreements (BPAs) and other existing contracts
- Provide documented acquisition requirements
- Avoid emergency and expedited procurements

Additional Information

- USDA customers must provide an approved Acquisition Approval Request (AAR) and other supporting information.
- Utilize other OCIO service offerings to minimize application integration efforts and reduce costs through economies of scale

NITC

NATIONAL INFORMATION TECHNOLOGY CENTER

"Partnering for Success"

Priority Matrix for Incidents and Service Requests

Determining Impact and Urgency

- **IMPACT:** A measure of the effect of an Incident, Problem, or Change on Business Processes (delivery of services)
    - **High -** Any Production application affected, or entire site, multiple systems/customers/applications, or critical infrastructure or support systems affected
    - **Medium –** Individual users or a small group of users affected. Non Production Incidents
    - **Low –** Routine requests with no customer or business impact

- **URGENCY**: A measure of the time available for repair or avoidance before impact is felt by business processes
    - **High –** Event impact is underway or imminent, and immediate and sustained action is required for resolution
    - **Medium –** Event scheduled or may occur but sufficient time remains to respond and prevent impact
    - **Low –** Event can be postponed or no specific completion time required

		Impact		
		High	Med	Low
Urgency	High	Critical	High	Med
	Med	High	Med	Low
	Low	Med	Low	Low

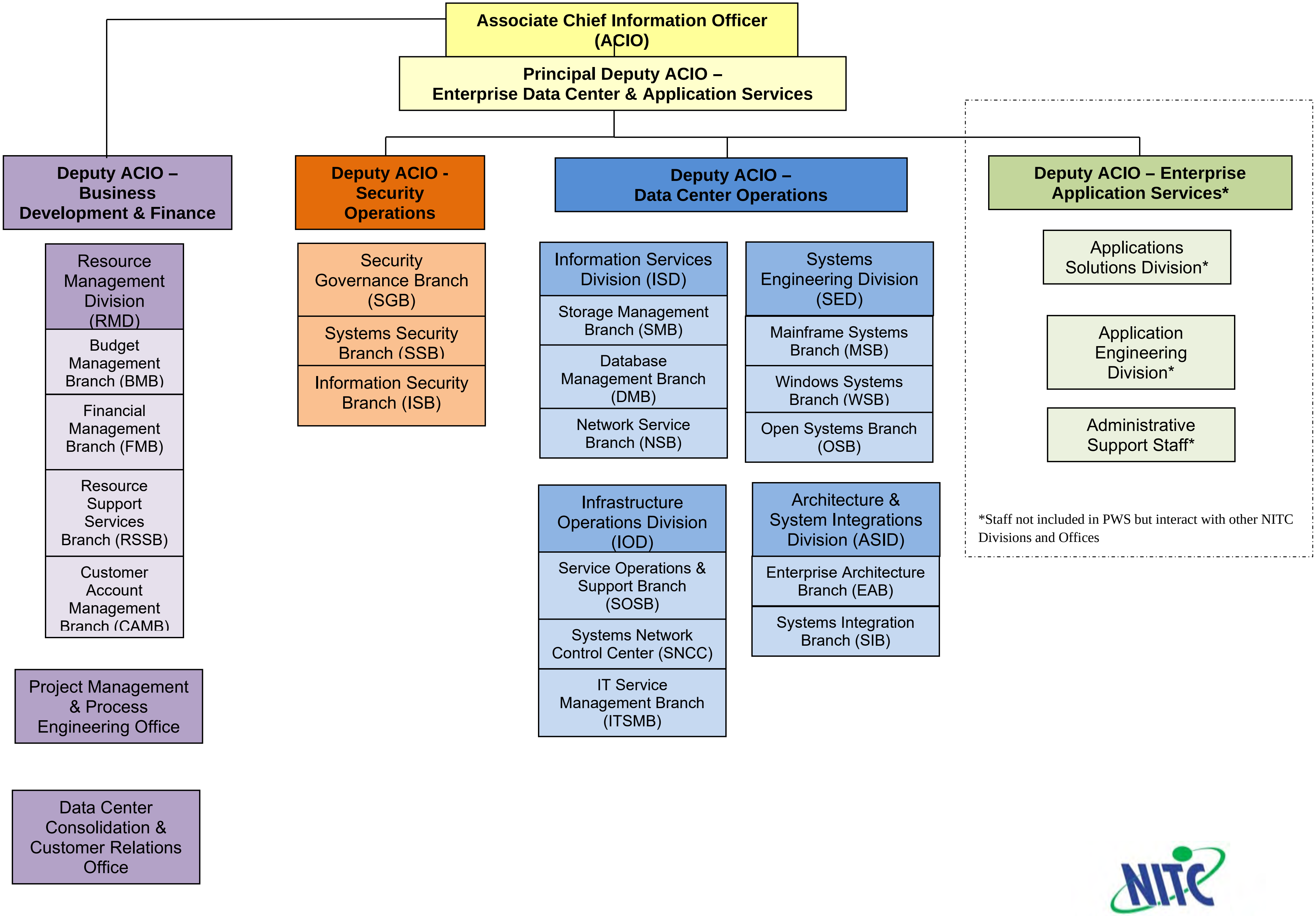
Priority Matrix for Incidents and Service Requests – cont.

- **Target Response Time** -Total timeframe in which an issue completes the following:
  - Detected/Reported and ticketed by the Service Desk
  - Ticket assigned and acknowledged and accepted by appropriate support personnel
  - **Escalation** – Tier1 has been unable to make contact with appropriate support personnel (*all members of the support group*) *AND* Target Response Time has been exceeded
    - **Primary Action** – Contact Support Group Branch Chief and inform him/her that you have been unable to make direct contact with his/her staff and require immediate assistance
    - **Secondary Actions** - Should *Primary Action* be unsuccessful, in order contact: Incident Manager, SOSB Chief, Support Group Division Director, IOD Director

- **Target Resolution Time** –Total time to service restoration or request fulfillment by NITC personnel.
  - **Escalation** – Tier2/Tier3 - have been unable to resolve the issue within the Target Resolution Time, or in the case of Tier 2 escalating to Tier 3, have been unable to make immediate contact with appropriate Tier 3 support personnel (*all members of the Tier 3 support group*)
    - **Primary Action** – Contact Support Group Branch Chief to inform him/her that the Target Resolution Time has been exceeded
    - **Secondary Action** - Should *Primary Action* be unsuccessful, contact the NITC Incident Manager or Incident Coordinator

Chart below shows the NITC Incident Management Priority Matrix with dashed lines representing escalation points. For purposes of Incident Management, business hours are defined from 6:00am – 6:00pm M-F.

PRIORITY	IMPACT	URGENCY					
		Target Response		Target Resolution			
		Tier 1		Tier 2		Tier 3	
CRITICAL	Widespread outage to NITC infrastructure. Customer production application or major application is down or seriously impacted. Immediate and sustained effort utilizing all available resources until resolved. Call-list proceedures activated	≤ 15 Minutes	Escalation	≤ 30 Minutes	Escalation	≤ 1 Hour	Escalation
		Immediate Phone Contact		Immediate Phone Contact			
HIGH	A single failure of a clustered or highly available environment Event Management alerts for production systems requiring action to avert potential disruption of service Immediate contact made to assess the incident	≤ 30 Minutes	Escalation	≤ 3 Hours	Escalation	≤ 4 Hours	Escalation
		Immediate Phone Contact		Immediate Phone Contact			
MEDUIM	Incidents and Event Management alerts for Non-Production Environments Incidents affecting individual users	≤ 1 Hour	Escalation	≤ 12 Business Hours			Escalation
LOW	Standard service requests, routine maintenance, and configuration changes Questions about accounts or contracts, information requests, and general feedback.	≤ 1 Hour	Escalation	≤ 5 Business Days			Escalation



Associate Chief Information Officer (ACIO)

Principal Deputy ACIO – Enterprise Data Center & Application Services

Deputy ACIO – Business Development & Finance

- Resource Management Division (RMD)
  - Budget Management Branch (BMB)
  - Financial Management Branch (FMB)
  - Resource Support Services Branch (RSSB)
  - Customer Account Management Branch (CAMB)
- Project Management & Process Engineering Office
- Data Center Consolidation & Customer Relations Office

Deputy ACIO - Security Operations

- Security Governance Branch (SGB)
- Systems Security Branch (SSB)
- Information Security Branch (ISB)

Deputy ACIO – Data Center Operations

- Information Services Division (ISD)
  - Storage Management Branch (SMB)
  - Database Management Branch (DMB)
  - Network Service Branch (NSB)
- Systems Engineering Division (SED)
  - Mainframe Systems Branch (MSB)
  - Windows Systems Branch (WSB)
  - Open Systems Branch (OSB)
- Infrastructure Operations Division (IOD)
  - Service Operations & Support Branch (SOSB)
  - Systems Network Control Center (SNCC)
  - IT Service Management Branch (ITSMB)
- Architecture & System Integrations Division (ASID)
  - Enterprise Architecture Branch (EAB)
  - Systems Integration Branch (SIB)

Deputy ACIO – Enterprise Application Services*

- Applications Solutions Division*
- Application Engineering Division*
- Administrative Support Staff*

*Staff not included in PWS but interact with other NITC Divisions and Offices

NATIONAL INFORMATION TECHNOLOGY CENTER

REQUEST FOR PROPOSAL
ID05140054

In Support Of

CLIENT AGENCY:

United States Department of Agriculture (USDA)
National Information Technology Center (NITC)

PROJECT TITLE:
Information Technology Support

~~Original Version dated December 18, 2014~~

Revision 1 dated January 23, 2015

Table of Contents

I. INTRODUCTION 3

A. Performance Based Contracting Approach 3

B. Period of Performance 3

C. Level of Support 3

II. MINIMUM REQUIREMENTS - READ THIS FIRST 3

III. INSTRUCTIONS TO CONTRACTORS 4

A. Submission of Proposal 4

B. General Contractor Instructions 4

IV. PROPOSAL CONTENT 5

A. General 5

B. Detailed 5

1. Cover Letter 5
2. Technical Capability 6
3. Past Experience and Performance 8
4. Price Submission 9

V. EVALUATION CRITERIA AND SELECTION PROCESS 9

A. General 9

B. Evaluation Factors 9

1. FACTOR 1: Technical Capability 9
2. FACTOR 2: Past Experience and Performance 10
3. FACTOR 3: Price 10

VI. SELECTION 10

A. Best Value Evaluation 10

B. Discussions and Competitive Range. 10

VII. ADDITIONAL TERMS AND CONDITIONS 10

VIII.RFP QUESTIONS 12

IX. DUE DATE 12

DATE:	January 23, 2015
MEMORANDUM FOR:	General Services Administration (GSA) Alliant Small Business (ASB) Governmentwide Acquisition Contract (GWAC)
FROM:	GSA Federal Acquisition Service (FAS) Acquisition Operations Division (5QZA) 1710 Corporate Crossing, Ste. #3 O'Fallon, IL 62269
SUBJECT:	Request for Proposal (RFP) for GSA Order Number ID05140054

I. INTRODUCTION

It is the intent of the GSA FAS 5QZA to issue a single-award task order against the GSA ASB GWAC to provide a full range of Information Technology (IT) services in support of the United States Department of Agriculture (USDA), National Information Technology Center (NITC).

A. *Performance Based Contracting Approach*

This RFP utilizes a Performance Work Statement (PWS) (**RFP Attachment 1**) to provide the Government's overall desired outcomes/objectives for this requirement. The PWS provides the overall scope and general requirements. Specific task requirements are identified in **PWS Attachment A** via the utilization of Contract Line Item Number (CLIN) descriptions. The performance standards and acceptable quality levels are identified in both PWS Attachment A and **PWS Attachment B**, Labor Hour CLIN Service Delivery Summary, as applicable.

B. *Period of Performance*

The resulting task order will have a one-year base period and four, one-year option periods.

C. *Level of Support*

For indicating the scope of work only, the estimated core initial staffing levels in terms of Full-Time-Equivalent (FTE) positions are identified in **PWS Attachment C**. It is anticipated that the workload will fluctuate based on fluid schedule requirements; therefore, the contractor shall include provisions for optional growth support throughout the task order life cycle as reflected in the pricing template, which includes lump sum labor allotments for optional growth support that are equivalent to a percentage of the price/cost for the core requirements. To ensure maximum flexibility with respect to the optional growth support, the contractor shall include a complete price list identifying the proposed hourly labor rates for all ASB labor categories (LCATs), as reflected in the pricing template, that will be used as the pricing basis for all optional growth support. The actual time frame for the optional growth support implementation will be dependent upon actual scheduling requirements.

II. MINIMUM REQUIREMENTS - READ THIS FIRST

Contractor proposals submitted in response to this RFP must comply with the following minimum requirements. Proposals that fail to meet any ONE of these minimum requirements may be eliminated from further consideration and deemed ineligible for award.

- Submit complete information as required in these instructions.
- Comply with all requirements identified in these instructions.

- As detailed in section III, all electronic documents/data submitted must be enabled so that the text/data in those documents/data can be searched, highlighted, copied and pasted into other documents/spreadsheets as needed.
- The contractor shall utilize and fully complete the required pricing template (**RFP Attachment 2**). Contractor proposed labor rates shall not exceed the applicable contract ceiling rates.
- The contractor shall complete the registration process (contractor company, contractor company representatives, and ASB contract) for GSA's web-based procurement system, Information Technology Solutions Shop (ITSS). Contractors may contact the ITSS Registration Helpdesk at 877-243-2889, option #2, for registration assistance.

III. INSTRUCTIONS TO CONTRACTORS

A. *Submission of Proposal*

1. Proposals shall be received no later than the date identified in paragraph IX. Proposals received after this time will not be considered for award. All proposals shall be uploaded to eBuy (www.ebuy.gsa.gov) under the applicable RFP. Regarding page limitations, the documentation shall be single-spaced, Times New Roman font (no exceptions), no smaller than 11 point type-size, no less than 1 inch margins, that (if printed) would fit on 8 ½ x 11 inch paper. The only exception to the paper size (not an exception to the font requirements) is for the price proposal and the organizational chart. The price proposal shall be printed on paper of a sufficient size to allow each sheet within the pricing template to be printed on a single page. The organizational chart shall be printed on paper of sufficient size to allow the entire chart to be displayed on a single page.

2. The acceptable electronic formats are Adobe PDF or Microsoft Word except for pricing. Price proposals shall be submitted using the required pricing template. All Adobe PDF documents and Microsoft Word documents shall be submitted with the ability to highlight and copy the text/data of the document. Any documents submitted that are protected in such a way which does not enable the ability to highlight/copy/paste the text/data will not be accepted. All Microsoft Word documents shall be fully readable by Microsoft Office version 2007.

3. Pricing proposal information shall not contain any technical proposal information and vice versa. When uploading the proposal to eBuy, separate all pricing and technical proposal information into separate zip (winszip.exe) folders. The naming convention for the WinZip folders shall be as follows: for pricing "GS-06F-XXXXX PRICING.zip", for Technical "GS-06F-XXXXX TECH.zip" (Complete the X's with the GSA ASB contract number). Submit the cover letter as a standalone document with the same style of naming convention "GS-06F-XXXXX COVER LETTER." All past performance information shall be included within the "GS-06F-XXXXX TECH.zip" file.

4. As stated in Section IX, hard copies are also requested. Timeliness and responsiveness of the proposasl is first determined by the submission of the electronic proposal in eBuy, then followed by the delivery of the hard-copy proposals. Hard copy proposals are to be delivered to the address listed in paragraph IX no later than 24 hours following the close date/time identified in the same paragraph. Failure to meet both the eBuy submission and hard-copy submission deadlines will remove the proposal from consideration. The electronic submission will serve as the "official" submission.

B. *General Contractor Instructions*

1. Proposals shall clearly demonstrate an understanding of each of the Government's objectives and requirements.

2. A complete proposal shall consist of a cover letter; a technical proposal, including both a technical capability section and a past experience and performance section; and a price proposal as detailed below. Incomplete proposals will not be further evaluated and deemed ineligible for award.

3. Proposals submitted in any other way except as detailed in the submission of proposals section above will not be further evaluated and deemed ineligible for award.

4. Any proposal or proposal modification will not be accepted after the due date and time for proposals.

5. Any assumptions forming the basis of the proposal, whether technical or price related, must be clearly identified in the applicable proposal.

6. All proposals shall be handled in accordance with FAR Subpart 3.104, Procurement Integrity.

7. Information requested herein must be furnished in writing and be fully and completely in compliance with RFP instructions. The information requested and the manner of submission is essential to permit prompt evaluation of all proposals on a fair and uniform basis. Simple statements of compliance without the detailed description of how compliance will be accomplished may not be considered sufficient evidence that the contractor can meet the technical requirements.

8. Contractor employees responsible for preparing material that may be procurement sensitive/proprietary data must mark each page that the contractor believes contains such information with the legend “Proprietary Data”.

IV. PROPOSAL CONTENT

A. *General*

1. Contractors should review the GSA ASB contract and are responsible for ensuring that proposals fully comply with all GSA ASB contract requirements. Each proposal shall clearly demonstrate that the contractor understands the PWS. The failure to explain the contractor’s ability to meet all requirements may result in the contractor's proposal not being considered. Clarity and completeness of proposals are of the utmost importance. Therefore, proposals must be written in a practical, clear and concise manner.

2. The narrative shall provide the Government with a reasonable assurance that the contractor has the relevant experience, capacity and capability required to meet or exceed the requirements and Government objectives identified within the PWS. A mere restatement of the PWS will be deemed unacceptable and may result in the contractor being eliminated from further consideration and deemed ineligible for award.

3. Each proposal shall be legible, single-spaced, typewritten Times New Roman font (no exceptions), no smaller than 11 point type-size, no less than 1 inch margins, which can be printed on 8 ½ x 11 inch paper (with the exception of the price proposal and organizational chart as per paragraph (III)(A)(1)). Overall proposal content, excluding the pricing submission, complete labor category skill level descriptions, and stand-alone cover letter, shall be no more than 45 pages in length.

B. *Detailed*

1. Cover Letter - An authorized official who can obligate the contractor shall sign a Cover Letter in contractor format, on contractor letterhead, demonstrating the contractor’s intent to be bound to the task order terms and conditions. This cover letter shall be no more than two (2) pages. The cover letter shall include:

   a) Alliant Small Business Contractor Company Name, Address, Contract Administration POC name/phone/email, Technical POC name/phone/email (if different than Contract Administration POC), CAGE, DUNS, TIN, Business Size, and GSA ASB Number.

   b) Subcontractor Information: The prime contractor shall also provide information on any subcontractor proposed. The cover letter shall identify and describe, in sufficient detail, any

proposed/potential sub-contractor agreements that may be required in the performance and completion of the task requirements.

2. Technical Capability (part of the technical proposal) - The written technical capability section of the technical proposal shall contain the following:

   a) Technical Approach

      i. Understanding and Methodology. The technical proposal shall include an overview of the methodology that will be utilized to guide the management and performance of the technical requirements identified in the PWS. The proposal shall include sufficient documentation to demonstrate both a detailed understanding of the stated requirements and the potential management challenges associated with the broad range of task areas involved. The technical proposal shall include a description of how the technical approach (i.e. description of the tasks to be performed) and analytical techniques will be applied to accomplish each of the requirements identified in the PWS.
      ii. Implementation. The technical approach shall include a phase-in plan to address the overall transition to the new task order, to include the recruitment and hiring of both new and incumbent contractor employees, and include sufficient documentation to demonstrate that the USDA will not experience a negative impact or disruption in service as a result from contractor personnel changes. The proposal shall identify all Government coordination that is anticipated to be required for the implementation. Detailed requirements for the phase-in plan are identified in PWS paragraph 8.7.1. If applicable, the phase-in plan shall clearly describe the contractor's proposed transition period, as defined in PWS paragraph 8.7.1., to include the following: specific duration of the transition period; detailed description of the proposed tasks to be completed during the transition period; and the identification of the resources proposed to complete such tasks during the transition period.

   b) Quality Control Plan (QCP). The plan shall include, but is not limited to the following:

      i. A description of the inspection system covering all services listed.
      ii. The inspection frequency.
      iii. The title of the individual(s) who shall perform the inspection and their organizational placement.
      iv. A description of the methods for identifying, correcting, and preventing defects in the quality of service performed before the level becomes unacceptable.

   c) Staffing Approach/Plan. The proposal shall include a complete staffing approach/plan that describes and illustrates the proposed utilization of contractor personnel resources and skill sets to perform and complete the PWS requirements. The staffing approach/plan shall include, at a minimum:

      i. An organization chart that depicts the complete staffing approach/plan and structure from the head of the company to all individual performers/positions (including key positions and non-key positions) proposed to support the resultant task order that demonstrates required personnel resources and skill sets via the identification of proposed labor categories for all individual performers/positions. The organization chart shall include the following:
         - A clear illustration of the operational relationships and task leadership among all entities, including all proposed joint venture team members and subcontractors, and the alignment of such entities. NOTE: The proposal shall include a narrative discussion identifying the roles and responsibilities of all proposed joint venture team members and subcontractors.
         - The identification of all proposed positions, to include the identification of all positions as either "key" or "non-key".

- The names of known individuals proposed to perform and fill positions. Positions to be filled by future identified proposed staffing shall be reflected by the use of "TBD" in lieu of a proper name.
- The United States (U.S.) citizenship status, if known, of all known individuals proposed to perform and fill positions. Positions to be filled by future identified proposed staffing shall also include such identification to illustrate the contractor's intent. In addition, the chart shall include the identification of the overall percentage, in numerical format, of proposed U.S. citizens and non-U.S. citizens.
- The name of the contractor company that will employ the individuals that staff all proposed positions.
- The identification of the physical locations for all proposed positions depicted on the chart.
- The identification of the proposed ASB labor category (LCAT) and PWS CLIN for all proposed positions.

ii. Resumes of proposed staffing for all key positions, which identify the education, certification, experience, background investigation status, and special skills of any individual(s) proposed to fill these positions as required by the applicable ASB LCAT. The resumes shall also include the identification of the experience, certifications, and expertise identified in the PWS as applicable and available. All resumes included within the proposal submission shall identify the proposed LCAT from the ASB contract and the PWS CLIN that the staffing member is being proposed to perform under.

iii. The identification of all proposed LCATs (for both key and non-key positions AND the known optional growth support) and complete skill level descriptions from the ASB contract and any additional task specific supplemental requirements in terms of expertise (i.e. education) and experience (in terms of years of experience) that are being proposed to support task order performance. NOTE: If it is determined that varying skill levels (i.e. entry level, journeyman, junior, intermediate, senior, etc.) are required to efficiently support task order performance and the ASB LCATs are not inclusive of such varying levels, the contractor shall supplement the contract level LCATs to provide varying levels as required. The proposed utilization of supplemental skill level requirements shall include the establishment of varying skill levels and the corresponding labor rates. In no instance shall the proposed labor rates for the varying skill levels of the LCATs exceed the established ASB ceiling rate for the subject LCAT.

iv. The identification and description of the contractor's policies regarding retention, recruitment and benefits, to include the items listed below, that will be applicable to resultant task order. The proposal shall clearly address the "consistency" of said policies as applicable to staffing plans that include the utilization of joint ventures and subcontractors.

- Description of plans, methods, procedures and personnel that will be used to recruit employees.
- Description of the standard compensation package(s) that will be employed, including benefits, work week policy, and overtime policy. The discussion regarding benefits shall address extended vacations (those exceeding a one week duration). The discussion shall also identify and describe any innovative features of the compensation package, such as unusual benefits or bonuses. In addition, if applicable, the discussion shall include a description and explanation for the potential utilization of a non-standard compensation package for specific positions. Such positions shall also be identified.
- Description of how the salary structure recognizes the distinct differences in technical and supervisory skills (where applicable) and the complexity of varied disciplines as well as job difficulty.
- Description of how and when training will be provided to ensure retention of employees and to ensure employees remain current on the required skills.
- Description of methods to ensure qualifications of prospective employees, to include contractor conducted background investigations.
- Explanation of what extraordinary measures of recruiting will be taken to fill critical positions requiring unique or hard-to-fill technical expertise and who will have the authority to incur the expense.

- A description of the orientation provided to the employee (at no cost to the Government) prior to assignment to the task order.

3. Past Experience and Performance (part of the technical proposal) - The written past experience and performance section of the technical proposal shall be composed of the following:

a) The Government will consider the relevance of past performance information obtained in relation to the scope of this procurement. Past Performance, either positive or negative, which is considered by the Government to be more closely related to the scope of this effort will be given additional weight in the evaluation process.

b) Description of three (a total of three to include subcontractor references – additional past performance references will not be considered for evaluation purposes) past project references that demonstrate successful experience in the type of work requested in the PWS. Each reference shall provide a thorough explanation of it's relevant to the PWS. Each reference shall include the information bulleted below and shall be no more than two pages in length. The performance references shall be within the last three years.

Furthermore, the ASB prime contractor is required to include (within the three references identified above) at least one project supporting a Federal Agency that the ASB prime contractor performed ~~and completed~~ as the prime with an annual value, for each annual period of performance included within the project, of no less than $2 million. If the ASB prime contractor is a Joint Venture (JV) company that has no relevant past/present performance, which shall be clearly stated within the proposal, then the Government may consider one reference from one partner of the JV to meet the requirement in the preceding sentence regarding minimum performance requirements as a prime contractor.

i. Contracting agency/company and technical points of contact with their phone numbers, electronic-mail addresses, and titles.
ii. Contract number and delivery/task order number, as applicable.
iii. Contract type.
iv. The original contract award date (for the base period of performance) and the completion (or estimated completion) date (shall reflect all option periods).
v. Contract value (value of each performance period shall be identified).
vi. Number of contractor personnel involved.
vii. Identification of on/off site performance locations.
viii. Scope of work.

c) If applicable, the submittal in this section shall also list any contract or purchase order under which either a cure notice or show cause letter was received, or any contract or purchase order that was terminated for cause by the Government within the past three years. The contractor must briefly explain the facts and circumstances in each such instance.

d) The contractor is to provide the Past/Present Performance questionnaire included in the RFP as Attachment 3 to all performance references identified in the contractor's technical proposal for completion and direct submission to the GSA as instructed within the questionnaire. The date established for receipt of the questionnaires will be the same as the date and time established for receipt of the RFPs.

e) The Government may supplement the information from the Government's Past Performance Information Retreival System (PPIRS) for the prime and any proposed subcontractor firms. The Government may contact members of the acquisition workforce involved with previously awarded Federal contracts. The Government's contact with other members of the Government acquisition workforce, including Contracting Officer's, Contracting Officer Representatives (CORs), and Project Managers, can provide valuable insight and supplement the written PPIRS evaluations or provide insight into the contractor's performance of ongoing contracts.

f) Offerors with no relevant past or present performance history shall receive the rating of "neutral" meaning the rating is treated neither favorably nor unfavorably.

4. Price Submission - Use of RFP Attachment 2 is required. The price submission, excluding RFP Attachment 2, shall not exceed five pages.

a) Format. The contractor shall utilize the Government provided template, in the Government provided file format.

b) Core and Optional Growth Support. For informational purposes only, the Government estimate included 1,920 labor hours as the basis for a FTE position.

c) CLIN Structure. The Government reserves the right to award the support for each CLIN on an individual basis, to include both a FTE basis and a fractional FTE basis, contingent upon funding availability.

d) The Government's future actions and uncertainty regarding continuing need may result in the requirement to reduce the duration of support provided via the FFP FTE positions or fractional FTE positions (if proposed). As such, the Government hereby reserves the right to reduce the firm fixed price amount for each position based on a prorated calculation.

e) Travel. The Government's estimated travel cost for each performance period is listed in the Government provided template. The proposal shall identify any indirect cost related to the travel other direct costs. The proposal shall include a copy of the Defense Contract Audit Agency (DCAA) approval letter for any indirect rates (i.e. G&A, etc.).

f) Un-scheduled (work hour category D) Support. The contractor shall clearly identify all costs, other than the standard billable labor hours expended by contractor resources in direct support of such requirements, associated with support provided under work hour category D. The contractor shall propose and clearly describe a cost effective approach. If there are no additional costs other than the standard billable labor hours expended by contractor resources in direct support of such requirements, the contractor shall clearly state and indicate such within the price proposal.

g) The period of performance dates identified in the PWS are estimated dates. The actual performance dates for the base period may require revision, resulting in an earlier or a later start date. Price proposal revisions will be not required or considered if a revision to the base period of performance is required. All of the performance periods (Base Period, Option Periods 1, 2, 3 and 4) will each be for a period of 12 months, with each option period of performance reflecting the subsequent 12-month period following the preceding period.

V. EVALUATION CRITERIA AND SELECTION PROCESS

A. *General*

1. Evaluations will be conducted in accordance with the FAR Part 16.505(b).

2. GSA will determine best value to the Government based on evaluation of price and non-price factors considered. However, the Government will not issue an award at a significantly higher evaluated price to achieve only slightly superior performance capabilities. GSA will verify that proposed services are consistent with the contractor's GSA ASB contract.

B. *Evaluation Factors*

1. FACTOR 1: Technical Capability - The written Technical Capability submission composed of the Technical Approach, QCP and Staffing Approach/Plan. The items listed under this Technical

Capability Factor ARE NOT sub factors and are not separately weighted for evaluation purposes. All items will be considered together for purposes of assigning a rating to this factor. The feasibility, extent, and quality of the contractor's technical capability will be evaluated based on the written submittal described in section IV(B)(2), above. The evaluation will be based on information pertaining to technical approach, and specifically focus on the breadth, depth and scope of the contractor's knowledge and understanding of the requirements described in this section. In addition, the relative quality and viability of the proposed staffing/labor mix/level of effort will be evaluated.

2. FACTOR 2: Past Experience and Performance - The Past Performance evaluation will include the references described in IV(B)(3), which may be verified by contacting references as deemed necessary by the Government along with past performance questionnaires, and will be evaluated based on the relevance of the information submitted. In rating this factor, GSA will consider the relevance in size and scope of each reference listed to the work described in this RFP. Past performance for projects similar in size and scope to the work described in this RFP may be given more weight in the evaluation. As such, the description of the work performed must be sufficiently detailed for the Government to make this determination.

3. FACTOR 3: Price – The Government will evaluate the realism and reasonableness of the proposed prices, rates, and number of labor hours, to determine overall best value. In addition, the Government will confirm that the rates proposed in the entire pricing proposal are accurate when compared to the contractor's current GSA ASB contract rates. Proposals containing inaccurate pricing information may be deemed ineligible for award and will not be further evaluated

VI. SELECTION

A. *Best Value Evaluation*

1. Proposals must demonstrate a clear understanding of the nature and scope of the work required. Failure to provide a realistic, reasonable, and complete proposal may reflect a lack of understanding of the requirements and may result in the proposal receiving no further evaluation and determined ineligible for award. Award will be established with the responsible contractor whose proposal conforms to the requirements outlined in this RFP and is most advantageous to the Government based on the best value determination.

2. The items listed under Technical Capability ARE NOT sub factors and are not separately weighted for evaluation purposes. All items will be considered together for purposes of assigning a rating to this factor.

3. The relative weights for the non-priced factors are listed in descending order of importance: Technical Capability and Past Experience and Performance. All non-priced factors combined are significantly more important than price.

4. Potential risk to the Government will also be evaluated. Technical and performance risk, based upon the proposer's evaluated technical capability and past performance experience, will be considered during the evaluation as well as any possible pricing risk and risks incurred as a result of the proposal assumptions.

B. *Discussions and Competitive Range*.

The Government intends to award a task order without discussion with respective contractors. The Government, however, reserves the right to conduct discussions if deemed in its best interest. The contracting officer may limit the number of proposals in the competitive range to the greatest number that will permit an efficient competition among the most highly rated proposals.

VII. ADDITIONAL TERMS AND CONDITIONS

The following clauses apply to this RFP and are provided by reference. The following clauses are incorporated with the same force and effect as if provided in full text:

FAR 52.212-4, Contract Terms and Conditions – Commercial Items (Dec 2014), Alternate I (May 2014)

FAR 52.217-5, Evaluation of Options (Jul 1990)

FAR 52.219-14, Limitations on Subcontracting (Nov 2011)

The following clauses are incorporated in full text:

FAR 52.217-8, Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor prior to expiration of the contract. (End of Clause)

FAR 52.217-9, Option to Extend the Term of the Contract (Mar 2000)

a) The Government may extend the term of this contract by written notice to the Contractor prior to expiration of the contract; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 60 months. (End of Clause)

GSA Special Clause: Limitation of Government's Obligation – Firm Fixed Price

Line items for Firm Fixed Price services may be incrementally funded. For these item(s), the sum of *** of the *** total price is presently available for payment and allotted to this task order award. An allotment schedule will be provided.

The Contractor agrees to perform up to the point at which the total amount payable by the Government, including reimbursement in the event of termination of those item(s) for the Government's convenience, approximates the total amount currently allotted to the contract. The Contractor is not authorized to continue work on those item(s) beyond that point. The Government will not be obligated in any event to reimburse the Contractor in excess of the amount allotted to the contract for those item(s) regardless of anything to the contrary in the clause entitled "Termination for Convenience of the Government." As used in this clause, the total amount payable by the Government in the event of termination of applicable contract line item(s) for convenience includes costs, profit, and estimated termination settlement costs for those item(s).

Notwithstanding the dates specified in the allotment schedule of this clause, the Contractor will notify the Contracting Officer in writing at least ninety days prior to the date when, in the Contractor's best judgment, the work will reach the point at which the total amount payable by the Government, including any cost for termination for convenience, will approximate 85 percent of the total amount then allotted to the contract for performance of the applicable item(s). The notification will state (1) the estimated date when that point will be reached and (2) an estimate of additional funding, if any, needed to continue performance of applicable line items up to the next scheduled date for allotment of funds identified in this clause, or to a mutually agreed upon substitute date. The notification will also advise the Contracting Officer of the estimated amount of additional funds that will be required for the timely performance of the item(s) funded pursuant to this clause, for a subsequent period as may be specified in the allotment schedule of this clause or otherwise agreed to by the parties. If after such notification additional funds are not allotted by the date identified in the Contractor's notification, or by an agreed substitute date, the Contracting Officer will terminate any item(s) for which additional funds have not been allotted, pursuant to the clause of this contract entitled "Termination for Convenience of the Government."

When additional funds are allotted for continued performance of the contract the parties will agree as to the period of contract performance which will be covered by the funds. The provisions of this clause will apply in like manner to the additional allotted funds and agreed substitute date, and the contract will be modified accordingly.

If, solely by reason of failure of the Government to allot additional funds, by the dates indicated below, in amounts sufficient for timely performance of the contract, the Contractor incurs additional costs or is delayed in the performance of the work under this contract and if additional funds are allotted, an equitable adjustment will be made in the price or prices (including appropriate target, billing, and ceiling prices where applicable) of the item(s), or in the time of delivery, or both. Failure to agree to any such equitable adjustment hereunder will be a dispute concerning a question of fact within the meaning of the clause entitled "Disputes."

The Government may at any time prior to termination allot additional funds for the performance of the contract.

The termination provisions of this clause do not limit the rights of the Government under the clause entitled "Default." The provisions of this clause are limited to the work and allotment of funds for the contract. This clause no longer applies once the contract is fully funded except with regard to the rights or obligations of the parties concerning equitable adjustments negotiated under this clause.

Nothing in this clause affects the right of the Government to terminate this contract pursuant to the clause of this contract entitled "Termination for Convenience of the Government."

Nothing in this clause shall be construed as authorization of voluntary services whose acceptance is otherwise prohibited under 31 U.S.C. 1342.

The parties contemplate that the Government will allot funds to this contract in accordance with the following schedule:

On execution of task order	***
Schedule To Be determined	***

*** To be inserted after negotiation/prior to task order award(s).
(End of clause)

VIII. RFP QUESTIONS

All questions resulting from the RFP shall be submitted in writing via e-mail to both individuals identified below no later than January 9th, 2015, 5:00 PM EST. All questions received will be consolidated and a response will be issued via a RFP amendment. Questions received after this date will not be considered

Yjuania Still	Wendi Borrenpohl
Contracting Officer	Project Manager
GSA/FAS	GSA/FAS
Phone: 618-622.5809	Phone: 618.622.5806
Email: yjuania.still@gsa.gov	Email: wendi.borrenpohl@gsa.gov

IX. DUE DATE

Electronic proposals must be submitted no later than the date established in the eBuy, with six hardcopies to be delivered no later than the first business day of this date/time, to:

GSA/FAS/5QZA
1710 Corporate Crossing, Suite 3
O'Fallon, IL 62269-3734

YJUANIA STILL
Contracting Officer

Attachments:
1. Performance Work Statement
2. Pricing Template
3. Past Performance Questionnaire

PERFORMANCE WORK STATEMENT

In Support Of

CLIENT AGENCY:

**United States Department of Agriculture (USDA)
National Information Technology Center (NITC)**

**PROJECT TITLE:
Information Technology Support**

~~Original Version dated December 18, 2014~~

Revision 1 dated January 23, 2015

Table of Contents

1. BACKGROUND ..... - 4 -
2. OBJECTIVE ..... - 4 -
3. SCOPE ..... - 5 -
4. APPLICABLE DOCUMENTS ..... - 5 -
4.1. Applicable Regulations and Documents ..... - 5 -
5. TASK REQUIREMENTS ..... - 6 -
5.1. Contract Line Item Numbers (CLINs) ..... - 6 -
6. PERSONNEL ..... - 7 -
6.1. General Requirements ..... - 7 -
6.2. CLIN Specific Experience and Expertise ..... - 7 -
6.3. Training ..... - 7 -
6.3.1. Contractor Staff Training ..... - 7 -
6.3.2. Seminars, Symposia, Or User Group Conferences ..... - 7 -
6.3.3. Mandatory Government Training ..... - 7 -
6.4. Personnel Retention and Recruitment ..... - 8 -
6.4.1. Work Transition Plan ..... - 8 -
7. QUALITY ..... - 8 -
7.1. Quality Control ..... - 8 -
7.2. Quality Assurance ..... - 9 -
8. DELIVERABLES ..... - 9 -
8.1. Contractor Submission ..... - 9 -
8.2. Government Review ..... - 9 -
8.3. Data and Deliverable Rights ..... - 9 -
8.4. Transfer of Ownership ..... - 9 -
8.5. Monthly Invoice ..... - 10 -
8.6. Monthly Status Report ..... - 10 -
8.7. Phase-In / Phase Out ..... - 10 -
8.7.1. Phase-In Plan ..... - 10 -
8.7.2. Phase Out Plan ..... - 11 -
8.8. Deliverable Matrix ..... - 11 -
8.9. Other Reporting Requirements ..... - 12 -
9. PERFORMANCE ..... - 12 -
9.1. General ..... - 12 -
9.2. Kickoff Meeting ..... - 12 -
9.3. Period of Performance ..... - 12 -
9.4. Place of Performance. ..... - 12 -
9.4.1. Applicability of Telework. ..... - 13 -
9.4.2. Travel ..... - 14 -
9.5. Hours of Work ..... - 14 -
9.5.1. Standard Duty Hours Support ..... - 14 -
9.5.1.1. Normal Workday - (work hour category A) ..... - 15 -
9.5.1.2. Staggered Workday - (work hour category B) ..... - 15 -
9.5.2. Non-Standard Duty Hours Support ..... - 15 -
9.5.3. Continuity of Operations (COOP)/Disaster Recovery (DR) ..... - 15 -
9.5.4. Holidays ..... - 16 -
9.5.5. Government Administrative Leave Situations ..... - 16 -
10. GOVERNMENT FURNISHED EQUIPMENT/INFORMATION/ACCESS ..... - 16 -

10.1. General - 16 -
10.2. Property - 16 -
10.2.1. Facilities - 16 -
10.2.2. Equipment at Authorized On-Site Federal Work Locations - 17 -
10.2.3. Facilities and Equipment at Remote Work Locations - 17 -
10.2.4. Materials - 17 -
10.2.5. Validation of Government Furnished Items (GFI) and Equipment Inventory - 17 -
10.3. Use of Government Property - 17 -
10.3.1. Desk Telephones - 17 -
10.3.2. Mobile/Wireless Telephones and Smart Devices - 17 -
10.3.3. Mail/Postage - 18 -
10.3.4. Electronic Mail (E-mail) - 18 -
10.3.5. Copiers - 18 -
10.3.6. Fax Machines - 18 -
10.3.7. Computer and Internet - 18 -
10.3.8. Canvassing, Soliciting, or Selling - 18 -
10.3.9. Security Violations Using Government Equipment - 18 -
10.4. Government Vehicles - 18 -
10.5. Return of Government Property - 18 -
10.6. Conservation of Utilities - 19 -
11. SECURITY - 19 -
11.1. United States Citizenship - 19 -
11.2. Security Awareness Training - 19 -
11.3. Background Investigation Requirements - 20 -
11.4. Access to Sensitive/Critical Data - 21 -
11.4.1. Non-Disclosure Agreement - 21 -
11.4.2. Data Access - 21 -
11.5. Security Incident Reporting - 21 -
11.6. Permanent Security Badge Requirements - 21 -
11.7. Display of Permanent Security Badges - 22 -
11.8. Temporary Security Badge Requirements - 22 -
11.9. Facility Security Requirements - 23 -
11.10. Parking Requirements - 24 -
12. ADMINISTRATIVE CONSIDERATIONS - 24 -
12.1. Government Representatives - 24 -
12.2. Procedures for Payment - 25 -
12.2.1. Performance Based Payment Percentages - 25 -
12.2.2. Submission - 25 -
12.2.3. Non-Compliance - 25 -
12.3. Personal Service - 25 -
12.4. Section 508 - 25 -
12.5. Privacy Act - 25 -

PERFORMANCE WORK STATEMENT (PWS)

1. BACKGROUND

The National Information Technology Center (NITC) within the Office of the Chief Information Officer (OCIO) is charged with offering cost competitive, cloud-based, automated data processing hosting services to USDA and other federal government organizations. The NITC generates operating revenue under a "fee-for-service(s)" model administered through USDA's working capital fund. NITC has grown in responsibility as the number of physical and virtual, mid-tier servers has grown based on customer demand. It is anticipated that the growth will continue. At the time of preparing this performance work statement, the NITC is supporting USDA customers and other federal government organizations as they strive to achieve the President's mandate to dispose of unneeded federal real estate and consolidate federal data centers.

The NITC provides comprehensive, cloud-based hosting services, associated operations, security, and professional support services to a customer base of 35 federal organizations. The Enterprise Data Center hosts business applications supporting millions of citizens across the United States of America. The NITC organization has been designated a USDA Enterprise Data Center with locations in Kansas City, MO; St. Louis, Missouri; Beltsville, Maryland; Washington, DC; Salt Lake City, UT; Fort Worth, TX; and Fort Collins, CO. The NITC has earned the title of a GSA FedRamp certified cloud service provider.

The NITC utilizes an IT Infrastructure Library / IT Service Management (ITIL/ITSM)-based framework to develop processes & policies for all work activity tracking, process management and workflow. The current ITSM automation suite is provided through BMC's Remedy COTS offering. The ITSM suite will generate task assignment queues. The policies and direction for many of these automated processes are directed by the Enterprise Change Control Board (ECCB) which governs the tool implementation. The contractor shall use this tool and adapt to the methods implemented by the NITC. During the course of this task order, the ITSM Remedy systems of the NITC and International Technology Services (ITS) organizations will continue to data share to provide unified responsiveness. It is anticipated that data sharing and ticket assignment will continue to be enhanced in the coming years.

The NITC also partners with the ITS to provide hosting and network solutions for USDA's Service Center Agencies (i.e., Farm Service Agency, Natural Resources and Conservation Service and Rural Development). This task order seeks to continue to improve those services that are provided through the use of Memorandum of Understandings (MOUs), Service Level Agreements (SLAs) and Operating Level Agreements (OLAs). The contractor shall to adhere to the language and conditions of these documents. Copies of all MOUs/SLAs/OLAs relevant to this task order that are in place at the time of award will be provided to the contractor. The MOUs/SLAs/OLAs facilitate the understanding of the separate but shared roles and responsibilities for services that are provided by the OCIO organizations.

2. OBJECTIVE

The objective of this task order is to provide Information Technology (IT) support services to complement in-house capabilities in order to meet the short and long-range plans of both USDA and non-USDA serviced agencies. Specific objectives include, but are not limited to, those identified below.

- **Objective 1** - The Contractor shall work as a part of the technical support team that the NITC leverages to provide world-class data center service offerings and professional services to the USDA and other federal government customers (i.e., customer base) and shall enable the increased visibility of NITC value-added benefits by meeting or exceeding service expectations. In the data center operational support context, the support team is comprised of vendor-dispatched hardware maintenance personnel; vendor specific hardware and software technical "hot-line" support personnel; federal employees, and contractor employees. Given the complexity of the data center hosting environment and the customer base's application software systems running on the hosting environment, system outages could require all or some of the support team, described above, to be mobilized to resolve the emergency.
- **Objective 2** - The Contractor shall support NITC data center officials in the completion of task assignments securing the availability, reliability and integrity of the data center through routine

operations & maintenance activities.

- **Objective 3** - The Contractor shall support NITC data center officials in the completion of work order priorities assigned through the ticketing system (i.e., NITC's implementation of BMC's Remedy COTS) and defined by the NITC Incident Management Process Guide. The contractor shall support incident, change and problem management and shall reinforce incident coordination and service metric tracking to staff.
- **Objective 4 -** The Contractor shall support NITC data center officials in the preparation of documentation for the NITC Change Control Board.
- **Objective 5 - T**he Contractor shall support NITC data center officials with the implementation of federal mandates and the seam-less coordination with other OCIO organizational units.
- **Objective 6** - The Contractor shall support NITC data center officials with a full range of back office functions for the budgetary, financial and administrative management of the center.
- **Objective 7** - The contractor shall ensure close coordination, communication, and resource sharing and shall support resolution, restoration, and root cause analysis to reduce mean time to repair and reduce the overall cost of operations and maintenance support.
- **Objective 8 –** The contractor shall support the achievement of long-term cost reduction by adapting ITIL best practices and applying automation to data center operations that reduce overall costs and better allocate resources.

3. SCOPE

The projects of the data center are national in scope and impact the United States economy. The scope of work for this PWS will cover a full range of functional areas and technical skill sets required to support the USDA, OCIO, NITC. The task order may include, but not be limited to, the IT support services for work to be accomplished using different computing environments that can include various hardware platforms, software, and telecommunications capabilities currently installed or planned to be installed by the NITC or customer agencies. This will require qualified personnel with expertise in computer equipment, software, and telecommunications facilities used in customer agency offices. The skill sets needed will vary depending upon the requirements.

USDA agencies are currently using, but are not limited to, the following types of hardware and software:

- NITC hardware and software include installed IBM-compatible mainframe computers, z/OS operating system with JES2 and VTAM, TSO, CICS, FOCUS, IDMS, and DB2.
- Other equipment currently in use includes SUN, HP, RISC based systems, and IBM-compatible PCs.
- Software currently in use includes ORACLE, S2K, SYBASE, C, SAS, COBOL, FORTRAN, UNIX, WINDOWS (200X), INFORMIX, DB2, Cold Fusion, Java, MS SQL, Adobe Acrobat, Adobe Photoshop, and Web Trends and other Web development tools, including WebSphere.

NITC supports multiple mainframe systems, several thousand mid-range systems, and various storage platforms. The current system environment includes: IBM, Sun, HP, and Intel-based servers with LINUX, AIX, Unix, HP-UX, Sun Solaris, Windows (9X, NT, and 200x), and Windows Data Center Operating systems, and storage solutions including Storage Area Networks. NITC offers multi-platform application, database support, and maintenance. Some of these include: High Availability Solutions, Mail/Directory Server Applications, Web Servers, and Database Applications.

NOTE: The above information is for general reference and subject to change. The IT environments at the NITC and customer agencies are dynamic and can change constantly.

4. APPLICABLE DOCUMENTS

4.1. Applicable Regulations and Documents

The following documents (versions current at time of award) are incorporated into the resultant task order award. Succeeding revisions may be substituted or incorporated as required. This list is not all inclusive and or limited to the following:

- http://wiki.edc.usda.gov/mediawiki/index.php/Main_Page.
- ACM-0015-01 - Human Resources Management Contractor In-Process Rev 2 (PWS Attachment D-1).
- ACM-0015-02 - Human Resources Management Contractor Exit Process Rev 2 (PWS Attachment D-2).
- Applicable NITC Directives that will be released after the resultant task order award.

5. TASK REQUIREMENTS

The contractor shall furnish all personnel, services, and supervision to perform the requirements of this task order. The contractor shall provide facilities and equipment for back office administration. Contractor employees shall clearly identify themselves as such at all times (badge display; identification announcement prior to or at the commencement of meetings and teleconferences; and correspondence including e-mail, etc.)

5.1. Contract Line Item Numbers (CLINs)

The specific task requirements to be completed under the below identified CLINs are included in PWS Attachment A, which includes the performance standards for the firm fixed price (FFP) CLINs. Additional performance standards for the labor hour (LH) CLINs are included in PWS Attachment B. Additional CLIN specific requirement information, presented in a summary display, is identified in PWS Attachment C.

CLIN Number	CLIN Title	CLIN Type
001	Audit Support Services	FFP
002	Budget Analysis Support Services	FFP
003	Business Continuity Planning Services	FFP
004	Enterprise IT Services Portfolio Management	FFP
005	Facilities Operations Services	FFP
006	Information Systems Security Support Services	FFP
007	ITSM Process Development and Documentation Services	FFP
008	ITSM Service Asset and Configuration Management Support Services	FFP
009	Program/Project Management Review Support Services	FFP
010	Task Order Management	FFP
011	Technical Architecture Support Services	FFP
012	Technical Writer	FFP
013	ADDM Administration & Modeling Services	LH
014	Application Integration Engineering Support Services	LH
015	Data Center Hardware Support Services	LH
016	Database Administration Services	LH
017	Mainframe Systems Programming Services	LH
018	Network Engineering Services	LH
019	Remedy Engineering and Administration Services	LH
020	Security Administration Services - AD & Identity Management	LH
021	Security Administration Services - MF Auth., Role Mgmt. & Access Cont.	LH
022	Security Engineering - Assessment Services	LH
023	Security Engineering - Monitoring, Detecting & Analysis Services	LH
024	Security Engineering - Network Access Control Services	LH
025	Senior Application Engineering Services	LH
026	Server Automation Tool Support Services	LH
027	Storage Administration Services	LH
028	Systems Administration Services	LH
029	Systems Monitoring Administration Services	LH

6. PERSONNEL

6.1. General Requirements

All contractor employees shall meet the minimum general requirements listed below.

- Strong written and oral communication skills in the English language. All contractor employees must be able to read, write, speak and understand English.
- Contractor personnel performing in a leadership capacity shall be capable of directing contractor personnel and interfacing with the Government and customers.
- Exceptional customer service skills.
- Strong time-management and prioritization skills.
- Ability to communicate applicable technical subject matter expertise to management and others.
- NITC follows the IT Infrastructure Library (ITIL) service operation best practices. It is important for the employees to demonstrate experience based on ITIL framework:
  - ITIL v3 foundation knowledge (or certification).
  - Ability to apply and provide feedback on service operation model and practices.

6.2. CLIN Specific Experience and Expertise

Documented experience and ability to demonstrate knowledge/skills/abilities with the required items (i.e. technologies, organizations, systems, processes, etc.) listed in the CLIN descriptions is required.

6.3. Training

6.3.1. Contractor Staff Training

The Contractor shall provide fully trained and experienced support staff for performance of the task order. Training of contractor personnel shall be performed at the Contractor's expense, except when the Government changes the requirements during performance of an on-going task and it is determined to be in the best interest of the Government. This will be negotiated on a case-by-case basis. Training at Government expense will not be authorized for replacement personnel nor for the purpose of keeping Contractor personnel abreast of advances in the state-of-the-art, or for training Contractor employees on equipment, computer languages, and computer operating systems that are available in the commercial market.

6.3.2. Seminars, Symposia, Or User Group Conferences

The Government will not authorize training for contractor employees to attend seminars, symposia, or User Group Conferences unless certified by the Contractor that attendance is mandatory for the performance of the task order requirement. When seminars, symposiums or User Group Conferences are authorized in writing by the COR, the Government will reimburse the Contractor for labor hours. The Contractor shall be responsible for expenses associated with the training, including, but not limited to, tuition, travel and per diem. This will be negotiated on a case-by-case basis

6.3.3. Mandatory Government Training

Mandatory Government training shall be tracked and monitored through USDA’s AgLearn system. A new contractor employee must complete security training before a log-on ID to USDA systems is issued. The contractor shall provide the information to the employee to review. The contractor will then proctor an exam that the contractor employee will complete and provide to the NITC COR. The NITC COR submits the exam to the NITC Federal Training Coordinator for exam grading. Once the contract employee passes the test they will be granted access to USDA systems, including AgLearn. If the employee is not successful in scoring a passing grade (70% or higher) on the first or second attempt, the contractor will be requested to submit a new candidate for the vacant position. Each contractor employee must complete annual training classes as mandated by USDA. The current mandatory courses include Security Awareness, Privacy Basics, and some positions require Role-Based Security training. These mandatory AgLearn courses can be completed through the AgLearn website free-of-charge. The COR shall notify the contractor of the training requirements and will provide the tools to complete this training. All required courses must be completed by the required dates by all contract employees. Mandatory government training classes may be completed during work hours. It is the intent of USDA to provide 30 calendar days written notice of annual training requirements to the Contractor's Task Order Manager. The Task Order Manager will be responsible for notifying subordinate contractor employees. In the event the contractor does not receive 30 calendar day notice, the contractor is still required to complete the training by the specified date(s).

6.4. Personnel Retention and Recruitment

The Contractor shall make every effort to retain personnel in order to ensure continuity until contract completion. If it should become necessary to substitute or replace personnel, the Contractor shall immediately notify the COR in writing of any potential vacancies and shall submit the resume(s) of replacement personnel within 14 calendar days of the notification. Additionally, for all new positions identified by the Government, the Contractor shall submit the resume(s) of proposed personnel within 14 calendar days of the Government's initial request. The Contractor shall submit the resume(s) of all potential personnel selected to perform under this task order to the COR through Information Technology Solutions Shop (ITSS) for Government review and acceptance/rejection. Upon Government acceptance of a personnel resume(s), the candidate shall be available to begin performance within 14 calendar days. The contractor shall ensure continuity of operations during periods of personnel turnover and long-term absences. Long-term absences are considered those longer than one week in duration.

6.4.1. Work Transition Plan

Due to the technical nature of the work and "least privilege" security access of user accounts, a situation could arise where work must be transitioned back to Government personnel upon a contract employee's departure from the workforce. In this situation, the contractor shall provide documentation in sufficient detail to allow for the transition of the workload to the Government. The Contractor shall provide documented processes that will serve as a basis for knowledge transfer and a historical record of the work accomplished. Documentation shall include a summary report on task requirements, contact information, and the location of documentation needed to provide continuity of service. This documentation must allow the Government to perform all tasks without the assistance of the Contractor.

7. QUALITY

Both the contractor and Government have responsibilities for providing and ensuring quality services, respectively.

7.1. Quality Control

The contractor shall establish and maintain a complete Quality Control Plan (QCP) to ensure the requirements of this contract are provided as specified in accordance with the applicable Inspection of Services Clause. The CO will notify the contractor of acceptance or required modifications to the plan. The contractor shall make appropriate modifications (at no additional costs to the government) and obtain acceptance of the plan by the CO. The Government has the right to require revisions of the QCP (at no cost to the Government) should the incorporated plan fail to deliver the quality of the services provided at any time during the contract performance. The plan shall include, but is not limited to the following:

- A description of the inspection system covering all services listed.
- The specification of inspection frequency.
- The title of the individual(s) who shall perform the inspection and their organizational placement.
- A description of the methods for identifying, correcting, and preventing defects in the quality of service performed before the level becomes unacceptable.

On-site records of all inspections conducted by the Contractor are required. The format of the inspection record shall include, but is not limited to, the following:

- Date, time, and location of the inspection.
- A signature block for the person who performed the inspection.
- Rating of acceptable or unacceptable.
- Area designated for deficiencies noted and corrective action taken.
- Total number of inspections.

7.2. Quality Assurance

The Government will perform periodic reviews of the contractor’s performance in accordance with the Government’s Quality Assurance Surveillance Plan (QASP). The Government reserves the right to review services to be provided, including those developed or performed at the Contractor's facilities, to determine conformity with performance and technical requirements. Government quality assurance will be conducted on behalf of the CO. The COR will be appointed to coordinate the overall quality assurance of technical compliance.

8. DELIVERABLES

Deliverables and due dates are identified in subsequent paragraphs.

8.1. Contractor Submission

Deliverables are to be transmitted with a cover letter, on the prime contractor’s letterhead, describing the contents, electronically through GSA’s web-based procurement system, ITSS, and to any other destination(s) as required per the Government’s request. The contractor shall provide hard copy deliverables as required per the Government’s request. All deliverables shall be produced using recommended software tools/versions as approved by the Government. All reports shall be accomplished utilizing the MS Office Software Suite to include MS Project as required.

8.2. Government Review

Government personnel will have 10 workdays to review deliverables (to include resubmissions) and provide written acceptance/rejection. The NITC USDA client representatives and/or the applicable COR(s) will notify the contractor of deliverable acceptance or provide comments in writing. The contractor shall incorporate Government comments, or provide rationale for not doing so within 5 days of receipt of comments. Government acceptance of the final deliverable will be based on resolution of Government comments or acceptance of rationale for non-inclusion. Additional changes volunteered by the contractor will be considered a resubmission of the deliverable.

8.3. Data and Deliverable Rights

All information such as software, data, designs, test materials, documents, documentation, notes, records, software tools acquired, and/or software source code and modifications produced by the contractor under this PWS shall become the sole property of the U.S. Government, which shall have unlimited rights to all materials and determine the scope of publication and distribution. The contractor shall be required to deliver electronic copies of all documents, notes, records and software to the Government upon termination of the task order or expiration of the task order. The Government shall retain ownership of all proprietary information and intellectual property generated under this task order.

8.4. Transfer of Ownership

All data and documentation, including all studies, reports, spreadsheets, software, data, designs, presentations, documentation, etc., produced by the contractor or for the Government using this PWS are the property of the Government upon its taking possession of task deliverables or upon termination of the task order or expiration of the task order.

8.5. Monthly Invoice

The contractor shall provide a monthly invoice to be submitted simultaneously with the monthly status report. Both documents shall be provided to applicable parties. The invoice and monthly status report shall be submitted as a single file. The components of the single file shall be arranged in the following order: accounting format invoice, monthly status report, and additional documentation as required.

The invoice shall include but not be limited to:

- Labor hours expended. The labor hours expenditure information shall include the identification of the employee name, labor category, hourly labor rate, and total number of labor hours expended.
- Supplemental Accounting Code Information. The invoice shall include a supplemental electronic file that includes the name of each contractor employee, the number of hours worked in the month associated with the NITC accounting/shorthand code associated with the work performed. PWS Attachment E is provided for informational purposes.
- Supporting documentation for travel costs. Invoices including travel costs shall include supporting documentation as required by the Federal Travel Regulation (FTR) (receipts for all costs $75.00 or greater). Invoice submissions including travel costs shall include completed travel expense sheets (i.e. travel voucher) for each trip for each employee.

8.6. Monthly Status Report

Monthly status reports shall include, but is not limited to, the items identified below.

- Status of task directives, schedules, deliverables. Status of task directives shall include a summary description and schedule of all task directives completed during the reporting period, all task directives currently on-going during the reporting period and all known task directives assigned for future reporting periods.
- current and cumulative task funding status (direct labor and travel funding status to be reported separately as required),
- outstanding issues, and proposed resolution approaches and actions to resolve any outstanding issues.
- Staffing report identifying current staffing roster, all current vacancies, and a record of all staffing departures
- Summary of the Scheduled Absence Calendar Availability deliverable for the two month period following the end of the MSR reporting period that clearly identifies and lists the scheduled absences
- Listing of all training to be completed within the two month period following the end of the MSR reporting period
- The monthly invoice shall be submitted simultaneously with the monthly status report.

8.7. Phase-In / Phase Out

8.7.1. Phase-In Plan

The contractor may or may not propose a separately priced transition period, for a duration to be determined and proposed by the contractor, but shall not exceed a period of 30 calendar days. The transition period is defined as the period of time (during the Phase-In) when the new contractor and the incumbent contractor will both be providing support to the client as required to support the transition to the newly awarded task order. If the contractor chooses to propose a transition period, such period shall be included and addressed within the below identified Phase-In Plan.

The Contractor shall develop a Phase-In Plan. Such Phase-In Plan shall present a clear understanding of the Phase-In tasks required, the issues likely to result from non-incumbent Contractor performance, and the Contractor’s proposal to resolve such issues. The Phase-In Plan shall include a clear and feasible strategy for delivering services required within the periods specified by the Plan and shall include a detailed plan-of-action and milestones to transition the functions identified in this PWS in a well-planned, orderly, and efficient manner. The Phase-In Plan shall include, at a minimum:

- Staffing plan.
- Development and submission of required deliverables.
- Interface with the Government and incumbent contractor (if applicable) during Phase-In, to include meetings or status reports, as required.
- Approach to maintaining quality and minimizing disruption during Phase-In.
- Development and dissemination of operating instructions, procedures, and control directives.

8.7.2. Phase Out Plan

During phase-out of this task order, which is determined to be a period of 90 days prior to the lifecycle end date of the task order, a smooth and orderly transition between the incumbent contractor and the successor contractor is necessary to ensure a minimum disruption to vital Government business. The Contractor shall cooperate to the extent required to permit an orderly changeover to the successor Contractor. The phase-out will be deemed completed by the COR when it is determined by the Government that the transition of property, data, and information developed as a part of this task order have been successfully changed over from the outgoing Contractor to the Government and the successor Contractor as required. Phase out activities include, but are not limited to, the tasks below.

- Submission of official comprehensive phase out plan.
- Daily communication of staffing status (i.e. projection of when incumbent contractor employees will off-board from the incumbent task order and identification of additional incumbent resources, such as a transition team, that may be needed to support the transition efforts) and overall phase out status, in accordance with the accepted phase out plan.
- Maintain the phase out schedule included within the phase out plan.
- Transition of property.
- Transition of supporting documentation.
- Transition of accounts (e.g. user accounts and user access).
- Knowledge transfer on the established installation, operation, and maintenance procedures of the technologies supported. The phase out plan shall clearly describe the proposed methodologies to be utilized for such transfer (e.g., written documentation, manuals, formal classroom type training, one-on-one training sessions, etc.).
- Execution and submission of phase out checklist, to include Government acceptance.

8.8. Deliverable Matrix

Title	Description	Due Date
Quality Control Plan.	Refer to PWS paragraph 7.1.	Submission due concurrent with contractor quote. If requested, a final QCP shall be furnished for acceptance by the GSA Contracting Officer addressing any Government comments provided no later than 30 calendar days after task order award.
Monthly Invoice.	Refer to PWS paragraph 8.5.	The 15th calendar day of the month following the reporting period.
Monthly Status Report.	Refer to PWS paragraph 8.6.	The 15th calendar day of the month following the reporting period.
Phase-In Plan (Transition Plan).	Refer to PWS paragraph 8.7.1.	Submission due concurrent with contractor quote. If requested, a final plan shall be furnished for acceptance by the GSA Contracting Officer addressing any Government comments provided no later than 15 calendar days after task order award.
Phase Out Plan.	Refer to PWS paragraph 8.7.2.	120 calendar days prior to the period of performance end date.
Project Specific Deliverables.	Plans, Reviews, Assessments, Reports, etc.	To be determined at the time the project specific task directive is assigned to the

		contractor.

8.9. Other Reporting Requirements

In addition to the deliverable requirements identified above, the contractor shall comply with the following:

- The contractor shall bring problems or potential problems affecting performance to the attention of the COR as soon as possible. Verbal reports shall be followed up with written reports, when directed by the COR, within 24 hours.
- The contractor shall provide, in writing to the COR, the results of all meetings with the client that affect and/or change conditions or result in additional agreements or requirements. The contractor shall not perform any work outside the scope or requirements of this PWS and resultant order without express written approval of the CO.

9. PERFORMANCE

9.1. General

Work is to be accomplished through the General Services Administration (GSA), Federal Acquisition Service (FAS), Great Lakes Region, through its task order with the contractor. Certification by the Government of satisfactory services provided is contingent upon the contractor performing in accordance with the terms and conditions of the referenced task order, this document, the approved technical and cost quotes, and all amendments. The client's representative, GSA's representatives, and the contractor's representative(s) shall meet when deemed necessary at the client’s request. The client representative, the GSA representatives, and the contractor’s representative may meet at the place determined by the client representative and GSA representatives.

9.2. Kickoff Meeting

Within 7 days of contract award, the Contractor shall initiate work on this task order by meeting with key client agency representatives, to include GSA, to ensure a common understanding of the requirements, expectations, and ultimate end products. The contractor shall discuss the overall understanding of the project and review the background information and materials provided by the client. Discussions will also include the scope of work, deliverables to be produced, how the efforts will be organized and project conducted; assumptions made/expected and results. A concerted effort shall be made to gain a thorough understanding of the client agency expectations. However, nothing discussed in this or in any subsequent meetings or discussions between the client and the Contractor shall be construed as adding, deleting, or modifying any task order requirements, including deliverable specifications and due dates.

9.3. Period of Performance

The anticipated period of performances are identified below. The actual periods may be adjusted based on the duration of the transition period, if applicable.

Transition Period:	June 1, 2015 through June 30, 2015 (maximum duration)
Base Year:	July 1, 2015 through June 30, 2016
Option Year 1:	July 1, 2016 through June 30, 2017
Option Year 2:	July 1, 2017 through June 30, 2018
Option Year 3:	July 1, 2018 through June 30, 2019
Option Year 4:	July 1, 2019 through May 31, 2020

9.4. Place of Performance.

The Primary Place of Performance shall be in NITC government facilities. When required by the Government, the Contractor shall also perform Task Order related activities at other Government and Contractor facilities within the local area. For the purposes of this Task Order, local area facilities are defined as those within 50 miles of a Primary Place of Performance. Reimbursement for local area travel shall not be authorized. Contractor requests for alternate performance locations (i.e. telework and work from other Government facilities) will be reviewed and considered on a case-by-case basis. The contractor shall obtain the required authorization prior to performing work at an alternate performance location. A list of the authorized NITC work locations are listed below. The work locations are subject to change.

a) Kansas City, Missouri (NITC-KC) Main Location:
USDA National Information Technology Center
8930 Ward Parkway
Kansas City, Missouri 64114-3363

b) St. Louis, Missouri Location at the Goodfellow Federal Complex:
United States Department of Agriculture
National Information Technology Center - STL
Goodfellow Federal Complex
4300 Goodfellow Blvd, Bldg. 104
St. Louis, Missouri. 63120

c) Washington, D.C. (NITC-DC) Location:
USDA National Information Technology Center
Room S-100, South Building
1400 Independence Avenue, S.W.
Washington D.C. 20250

d) Ft. Collins, Colorado Location:
USDA
Building A
2150 Centre Avenue
Fort Collins, Colorado 80526

e) George Washington Carver Center (GWCC), Maryland Location:
USDA National Information Technology Center
George Washington Carver Center
5601 Sunnyside Ave.
Beltsville, Maryland 20705-5000

f) Salt Lake City, Utah Location:
USDA-FSA-APFO
2222 West 2300 South
Salt Lake City, Utah 84119-2020

g) Ft. Worth, Texas Location:
Fort Worth Federal Center
501 West Felix Street, Building 23
Fort Worth, Texas 76115

9.4.1. Applicability of Telework.

All work performed at locations other than those identified as Government and/or contractor facilities shall be approved prior to performing the work. Federal contractors are not governed by Office of Personnel Management (OPM), GSA, or the individual agency policies; however, this does not prohibit contract employees from actually working at an alternate site, when/as appropriate **and specifically authorized by the Government**. Contractor shall develop telework policies to comply with the following requirements and address at a generic level within their Quality Control Plan. Alternate work arrangements for contractors shall be negotiated with the contractor's own employer and the appropriate agency official, to ensure policies and procedures are in close alignment and there is a clear and concise arrangement documenting the agreement. It remains the contractor's responsibility to ensure the services are performed in accordance with the terms and conditions of the award. The following are applicable telework classifications included within PWS Attachment C:

- No – No telework available.
- Situational – Occasional, pre-arranged telework.
- Limited – Specified number of days per week for telework.

9.4.1.1. Quality Control

The contractor shall address the pertinent facts impacting performance and ensure all affected contractor resumes reflect the applicable work site. The contractor shall provide justification to the Government when identifying and submitting an individual as a telecommuter and address implementation processes and procedures within the quality control plan. The contractor shall be responsible for ensuring the Government has the required access/details necessary for the Government to perform quality assurance responsibilities.

9.4.1.2. Compliance

The contractor shall comply with all agency security telework policies. The contractor shall ensure all services provided from an alternate site comply with the Federal Information Security Management Act of 2002 (FISMA) and address the following, as a minimum:

- Controlling access to agency information and information systems;
- Protecting agency information (including personally identifiable information) and information systems;
- Limiting the introduction of vulnerabilities;
- Protecting information systems not under the control of the agency that are used for teleworking;
- Safeguarding wireless and other telecommunications capabilities that are used for teleworking; and
- Preventing inappropriate use of official time or resources that violates subpart G of the Standards of Ethical Conduct for Employees of the Executive Branch by viewing, downloading, or exchanging pornography, including child pornography.

9.4.2. Travel

The Contractor shall also perform non-local travel in support of this Task Order, as required by the Government. The COR, or the appointed representative, shall have sole authority to approve non-local travel requests necessary to support Task Order performance. Not later than 5 business days prior to the Contractor's estimated date of departure, the Contractor shall submit to the COR, via ITSS, a travel request, to include travel justification, the proposed itinerary, and cost estimates for such travel. Federal Travel Regulations apply. The Contractor shall be responsible for all travel arrangements including airline, hotel, and rental car reservations. The Contractor shall make every commercially reasonable effort to schedule travel far enough in advance to take advantage of reduced airfares.

9.5. Hours of Work

The NITC is a shared services hosting provider (i.e., data center) that operates 24x7x365. Hours of support can and will be dependent on data center customer requirements for assigned tasks. The contractor shall coordinate work schedules with the COR to ensure service requirements are met, Government personnel are available, and customer results are achieved. The Contractor shall not exceed the monthly allocation of hours, calculated at 8 hours per day times the number of business days/month, without authorization from the COR. Additional details are provided below and the applicable work hour category for each CLIN is identified in PWS Attachment C**.**

9.5.1. Standard Duty Hours Support

The contractor shall provide for normal (during core business hours) and staggered standard duty hours support as required to ensure adequate coverage for US time zones.

9.5.1.1. Normal Workday - (work hour category A)

A standard normal workday is defined as any 8 hours of productive labor which must include the Core Business hours of 9:00 AM through 3:00 PM local time, Monday through Friday, excluding Federal Holidays. Exceptions may be required and shall be coordinated with the COR, to include short-term or long-term requirements for staggered workdays.

9.5.1.2. Staggered Workday - (work hour category B)

A standard staggered workday requires that on-site support shall be provided 6:00 AM through 6:00 PM local time, Monday through Friday, excluding Federal Holidays. Exceptions may be required and shall be coordinated with the COR, if coverage is required outside the 6:00 AM – 6:00 PM timeframe.

9.5.2. Non-Standard Duty Hours Support

The contractor shall provide for scheduled (planned work hours) and un-scheduled (other than planned work hours), non-standard duty hours support as required. The contractor shall identify a primary and alternate point of contact for non-standard, un-scheduled duty hours requirements. To ensure the applicable labor hours allocations are not exceeded (typically 40 hours per week), labor hours expended in support of non-standard duty hours requirements shall be off-set by reducing the number of standard duty work hours by an equivalent number. **The off-set shall be completed within the same monthly reporting period, unless the non-standard duty work hours are expended in the last week of the monthly reporting period. Non-standard duty work hours expended within the last week of the monthly reporting period shall be off-set within the first two weeks of the following reporting period.**

9.5.2.1. Scheduled (work hour category C)

Scheduled non-standard duty hours support shall be coordinated with the authorized Government point of contact and the contractor’s designated point of contact. Customers may request non-standard duty hours support for their environments (usually quarterly and during peak release or operational periods). Scheduled non-standard duty hours support may also be required to support a short term surge in requirements.

9.5.2.2. Un-Scheduled (work hour category D)

The Government may also request that the contractor provide un-scheduled (e.g., emergency technical support), non-standard duty hours support. The contractor shall respond within 15 minutes of notification. When off-site support can resolve the issue, the contractor’s personnel shall begin immediately upon notification. The contractor shall assess the cause, determine the scope of the problem, advise the appropriate Government organization, provide an estimated restoration time, and identify and implement action for problem resolution. When required, on-site support shall begin within one hour of notification to the contractor’s designated individual. This unscheduled support may include:

- Remote telephone support with the Government Technical Staff and/or customers.
- Remote support on GFE. Contractor employees may be equipped with GFE that enables remote data center access/log-on. The Government will not incur any costs associated with home-based WiFi or LAN access to the Internet.
- Onsite support.

9.5.3. Continuity of Operations (COOP)/Disaster Recovery (DR)

The National Security Presidential Directive/NSPD-51/Homeland Security Presidential Directive/HSPD-20, National Continuity Policy, requires Federal departments and agencies to maintain a comprehensive and effective continuity capability, including a Continuity of Operations (COOP) program. The COOP program, which also includes pandemic preparedness, ensures the continuation of essential functions under emergency situations.

An emergency may require personnel to temporarily relocate to a pre-designated, alternate work site or telework to ensure continuity of essential functions. A contract position may support the NITC's COOP plan, and the contractor may be required to report for work to assist the NITC federal staff in supporting critical business functions following a formal disaster declaration. Contract employees, under this scenario, are required to deploy to the alternate work site within 12 hours of COOP Plan activation for the support of government identified essential functions. The deployment to the alternative work site may last for up to 30 days. Travel and per diem expenses, if required, will be reimbursed in accordance with the Federal Travel Regulation (FTR).

NITC will also engage in "PLANNED" Disaster Recovery Exercises throughout a given Fiscal Year. As these exercises are typically planned well in advance, NITC may require contract employees' participation in these exercises after appropriately coordinated advance notice. There may also be the limited possibility of an "UN-PLANNED" Disaster Recovery Exercise. Unplanned exercises are typically conducted during business hours and NITC may require contract employees' participation after immediate notice. Travel is not expected to be required during DR Exercises/testing.

9.5.4. Holidays

The contractor is hereby advised that government personnel observe the following holidays: New Year's Day, Martin Luther King's Birthday, President's Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veteran's Day, Thanksgiving Day, and Christmas. In addition to the days designated as holidays, the government may observe the following days: any other days designated by Federal Statute; any other days designated by Executive Order; and any other days designated by the President's Proclamation. This includes Inauguration Day (Washington, D.C. metropolitan area only). Observance of such days by government personnel shall not be a reason for an additional period of performance, or entitlement of compensation. In the event the contractor's personnel work during the holiday, no form of holiday or other premium compensation will be reimbursed either as a direct or indirect cost.

9.5.5. Government Administrative Leave Situations

When the agency grants administrative leave to its employees, on-site assigned contractor personnel may be dismissed by the contractor. The contractor agrees to continue to provide sufficient personnel to perform task orders already in operation or scheduled, and shall be guided by the instructions issued by the COR. The Government will not pay for the labor hours during the leave granted to contract personnel as a result of inclement weather, potentially hazardous conditions, explosions, and other special circumstances.

10. GOVERNMENT FURNISHED EQUIPMENT/INFORMATION/ACCESS

10.1. General

The Government shall provide, without cost, the facilities, equipment, materials and services listed below. The Government furnished property and services provided as part of this task order shall be used only by the contractor only to perform under the terms of this task order. No expectation of personal privacy or ownership using any USDA electronic information or communication equipment shall be expected. All property at Government work sites, except for contractor personal items will be assumed to be government property unless an inventory of contractor property is submitted and approved by the CO/COR. Contractor personal items do not include computers, external drives, software, printers, and/or other office equipment (e.g., chairs, desks, file cabinets). The contractor shall maintain an accurate inventory of Government furnished property.

10.2. Property

10.2.1. Facilities

The Government will provide facilities at the authorized work locations specified in the task order. Use of the facilities by contractor employees will include all utilities, telephone, janitorial services and furniture for contractor employees performing tasks. The Government will provide the contractor access to buildings as required, subject to the contractor's employees obtaining the required security clearances.

10.2.2. Equipment at Authorized On-Site Federal Work Locations

The Government will provide the following at authorized on-site Federal work locations:

a) A suitable work environment (i.e., telephone, office space and furniture).
b) A personal computer/laptop and auxiliary hardware and software required in the performance of the task order.
c) Network connectivity required to perform work assignments. Network and computer access rights commensurate with work assignments.
d) Pagers, headsets, cell phones and maintenance agreements for such equipment when determined to be applicable by the COR. The Government will replace items that are determined to be beyond economical repair by the COR unless damage or loss is determined to be due to contractor negligence.

10.2.3. Facilities and Equipment at Remote Work Locations

When work from a remote location is authorized by the COR, the contractor will not be reimbursed for costs associated with remote connectivity from cell phones, WiFi access or Internet connection.

The contractor shall be responsible for ensuring the contractor employee has an adequate and safe office space that sufficiently protects Government equipment and information from loss, theft or unauthorized access. The contractor shall establish a telework agreement with the contract employee. The agreement, given a minimum of 24 hours of advanced notice, shall allow periodic inspections of the alternate work location can be undertaken. The purpose of the inspection is to ensure proper maintenance of Government-owned property and worksite conformance with safety standards and other specifications. The contractor is informed that telework is not a substitute for dependent care (i.e., child care or elder care) and that the appropriate arrangements must be made to accommodate children and adults who cannot care for themselves, while performing official duties of this contract at an alternate work location.

10.2.4. Materials

The Government shall furnish basic reference manuals, and any revisions, updates, and changes thereto for use by the contractor necessary to perform work assignments under the task order.

10.2.5. Validation of Government Furnished Items (GFI) and Equipment Inventory

The contractor shall develop and maintain a complete GFI inventory that shall be made available to the Government upon request. Within three (3) work days of receipt of any GFI, the contractor shall validate the accuracy of the materials and notify the COR, in writing, of any discrepancies.

NOTE: Validation shall consist of the Contractor checking for physical and logical completeness and accuracy. Physical completeness and accuracy shall be determined when all materials defined as Government furnished are provided, as defined in the task ordert. Logical completeness and accuracy shall be determined when all materials defined and associated with a program, system, or work package are provided.

10.3. Use of Government Property

10.3.1. Desk Telephones

Government telephones are provided for use in conducting official business. Contractor employees are permitted to make calls that are considered necessary and in the interest of the Government. The contractor will follow the same USDA and NITC policies as Government personnel the govern telephone usage.

10.3.2. Mobile/Wireless Telephones and Smart Devices

Government issued mobile/wireless telephone and smart devices may be assigned to contractor employees when the Government determines it is in the Government's best interest. Contractor employees are prohibited from using any Government issued device for personal use and would be subject to paragraph 10.3.9.

10.3.3. Mail/Postage

Contractor employees shall not have their personal mail directed to Government offices or use Government-furnished postage for personal benefit. The contractor shall follow the same USDA and NITC policies as Government personnel that govern mail usage including overnight delivery.

10.3.4. Electronic Mail (E-mail)

All Government e-mail access and use by contractor employees shall be in support of the individual's official duties and task responsibilities. All information that is created, transmitted, received, obtained, or accessed in any way or captured electronically using USDA's e-mail systems is the property of the Government. Contractor employees shall have clear identification in their e-mail signature block that identifies themselves as contractor employees in support of USDA NITC. Contractor employees are prohibited from forwarding e-mail generated from a Government provided e-mail account to personal mobile devices.

10.3.5. Copiers

Copiers are to be used to copy material for official Government business only in the performance of the tasks in this task order.

10.3.6. Fax Machines

Contractor employees shall not use fax machines for other than official Government business in the performance of the tasks in this task order.

10.3.7. Computer and Internet

All Internet and electronic media access accomplished by contractor employees (utilizing Government furnished equipment) shall be for official Government business in the performance of the tasks in this task order.

10.3.8. Canvassing, Soliciting, or Selling

Contractor employees shall not engage in private activities for personal gain or any other unauthorized purpose while on Government-owned or leased property, nor may Government time or equipment be utilized for these purposes.

10.3.9. Security Violations Using Government Equipment

Any contractor violating USDA security policies, guidelines, procedures, or requirements while using Government equipment or while accessing the USDA network may, without notice, have their computer and network access terminated, be escorted from their work location, and have their physical access to their work location removed at the discretion of the CO/COR. The CO/COR will notify the contractor of the security violation and request immediate removal of the contract employee.

10.4. Government Vehicles

The use of Government-furnished vehicles is NOT authorized under this task order, unless specific authorization is provided at the time of the proposed utilization. If a vehicle is needed to perform required services, it must be supplied by the contractor for their employees' official government business needs. This paragraph is not applicable to rental vehicles utilized during approved travel under the contract.

10.5. Return of Government Property

All Government property, data, software, information, documentation and equipment whether furnished by the Government to the contractor, created by the contractor, or acquired by the contractor with Government funding is property of the Government and shall be delivered/transmitted to the COR upon termination or expiration of the task order or per instructions from the CO.

10.6. Conservation of Utilities

The contractor shall instruct employees in utilities conservation practices. The contractor shall be responsible for operating practices that preclude the waste of utilities, which shall include:

a) Lights shall be used only in areas where and when work is actually being performed.
b) Mechanical equipment controls for heating, ventilation, and air conditioning system shall not be adjusted by the contractor or by contractor employees.
c) Water faucets or valves shall be turned off after the required usage has been accomplished.

11. SECURITY

USDA/OCIO has established legal and regulatory requirements that must be met before access is granted to federal IT resources. In order to gain access to USDA computer networks and computers, contractor personnel are required to initially complete the following requirements including, but not necessarily limited to:

- The USDA Information Security Awareness and Rules of Behavior training (web or paper-based). Additional and/or different courses may be required as USDA and NITC security policies change.
- The instructions to obtain USDA E-Gov access (eAuthentication).
- The documentation required for a security background investigation, which includes the Federal Bureau of Investigation's (FBI) National Criminal History Check ("fingerprint check") and eQIP.
- Information needed to obtain a Personal Identity Verification (PIV) card.

The contractor shall be responsible for ensuring compliance by its employees with all applicable federal regulations, to include those of GSA, NIST, USDA and HSPD-12. Contractors and their employees are subject to all Federal laws applicable to Government installations and are under the jurisdiction of the Federal Protective Service (FPS). The NITC COR, in conjunction with the USDA-OCIO Personnel Security Specialist (PSS), will ensure that the contractor submits the required Security Background Investigations/Clearances.

In addition, the contractor shall be responsible for ensuring compliance by its employees for any annual security training and reporting requirements of GSA, NIST, USDA and HSPD-12. Any contract employee working under this OCIO/NITC task order will be expected to follow the process for obtaining access to systems and notifying the Government for the termination of access upon the completion of performance under this task order. The contractor shall inform the COR and other designated NITC personnel if any changes are made in the status of contractor employees that would impact his/her access to USDA computer systems, and to follow the correct protocol for the creation, expansion and/or termination of such access.

11.1. United States Citizenship

No less than 75% of the contractor personnel assigned to this task, specifically to provide direct CLIN support, shall be United States citizens.

11.2. Security Awareness Training

Contract personnel who have access to USDA networks and computers will be required to take all security training necessary as determined by the Government to maintain access to the USDA network and computers. Currently, this includes an annual two hour or less, web-based Information Security Awareness training module and specialized training depending on the job function. The security training exam must be passed prior to any computer-system accesses are granted. Prior to an employee start-date, a paper-based exam must be administered by the contract site manager. If the employee is not successful in scoring a passing grade (70% or higher) on the first or second attempt, the contractor will be requested to submit a new candidate for the vacant position.

As USDA security policy changes, additional and/or different courses may be required. Contractor roles and permissions will be reviewed by the Government with the same frequency and at the same level as Government employees. Access to Government facilities, networks, and computers will require contractors to follow all Government mandated security alerts, procedures, patches and upgrades.

11.3. Background Investigation Requirements

After proper submission of paperwork, the Government covers the costs of investigations and submits the investigation for processing of all required security investigations/clearances, unless identified differently within this section. The scope of the security/background check required and the forms to be completed shall be determined in accordance with the Common Identification Standard for U.S. Department of Agriculture Employees and Contractors, USDA Directive 4620-002. The Government sponsor for this process shall be the COR or Government representative appointed in writing by the CO. The contractor shall be responsible for the preparation and submittal of the required forms. The contractor personnel shall not be required or permitted to perform work prior to receipt of the required security approvals.

Prior to being engaged on this task order, the contractor’s employee must first have been processed for a favorably adjudicated FBI fingerprint check. An unfavorable FBI fingerprint check will require that the contractor remove the employee from any further consideration pertaining to this task order.

The contractor should be aware of any of its employees possibly having had a background investigation through another government agency. The investigation, if verifiable by the Government and completed within the last 5 years, can be accepted by the Government in lieu of a FBI fingerprint check.

Fingerprinting Instructions: The COR will provide contact information to make arrangements for fingerprinting of the contractor employees. Fingerprinting instructions include:

- fingerprinting for Kansas City, MO based personnel can be accomplished by the Personnel Security Office (PSO) at 8930 Ward Parkway.
- fingerprinting for DC-based personnel can be accomplished by the PSO Assistant, at the USDA South Building or personnel at the Beltsville, Maryland data center; or,
- fingerprinting can be obtained from the local law enforcement agency after the PSO provides the fingerprint cards. The contractor shall pay for all costs of fingerprinting by local law enforcement agencies.

Background Investigations:
Assuming a prior favorable FBI fingerprint check has been verified, for taskings and task assignments that exceed 180 days in length, a full background investigation, processed through the Office of Personnel Management (OPM), will be required for all contract employees under this contract.

The background investigation, prior to being submitted to OPM, must be favorably reviewed at the local level by the PSO. The COR, working with the PSO, will determine what level of background investigation is required, based on the type and sensitivity of the duties and/or systems being accessed by the contractor. Current NITC policy requires processing of high-risk, public-trust investigations.

The Contractor is responsible for the immediate removal of employee(s) from the task order, if any person is identified as being a potential threat to the health, safety, security, general well-being, or operational mission of the USDA and its population. Additional items revealed in the background check that may be unacceptable are: conviction of a felony, a crime of violence or serious misdemeanor, a record of arrests for continuing offenses, adverse financial issues, or falsification of security documentation. As a reminder, an unfavorable FBI fingerprint check will eliminate a contractor’s employee for further consideration under this task order. Additionally, if unfavorable information is noted on the security questionnaire or developed during the ongoing or final background investigation, the Government retains the right to have the employee immediately removed from the task order at the Government’s discretion. Unless otherwise directed by the Contracting Officer, the contractor shall provide a replacement within ten (10) business days. New hires or substitute personnel are subject to the same security background requirements.

Special Procedures when the Data Center proper is the Primary Duty Station.

If a contractor's duty position at an NITC facility is located within the data center space, the additional provisions of NITC Directive A8 must be adhered to. Primarily, the contractor shall be required to have an investigation at the BI level. In addition to the favorable FBI Fingerprint check, the contractor must complete the online security questionnaire portion of the BI level investigation, which must then be favorably reviewed at the local level by the PSO's office. The online security questionnaire process must be initiated by the PSO and involves the use of the eQIP (Electronic Questionnaire for Investigation's Processing) system. Data center access cannot be approved until the online security questionnaire portion of eQIP has been completed, and the NITC Director or designee has approved the access.

11.4. Access to Sensitive/Critical Data

Contractor access to data deemed sensitive and/or critical by the Government will follow guidelines set forth in FIPS Publication 199, USDA and NITC security policy and only following successful completion of all security training.

11.4.1. Non-Disclosure Agreement.

Due to the sensitive nature of the data and information being worked with on a daily basis, all Contractor personnel assigned to the Task Order are required to complete the Government provided non-disclosure agreement within 15 calendar days after Task Order award, or prior to task order assignment, to ensure information that is considered sensitive or proprietary is not compromised. Signed non-disclosure statements shall be provided to the COR.

11.4.2. Data Access

The contractor may be required to have access to live production data for the performance of this task order. Any records and data or information the contractor may have access to may be highly sensitive and confidential. The contractor shall not divulge or missuse any information about files, data processing activities or functions, user IDs or passwords, or any other knowledge that may be gained, to anyone who is not authorized to have access to such information. It is the contractor's responsibility to ensure that other persons have the proper authorization

11.5. Security Incident Reporting

Contractors shall report the loss or suspected loss of equipment or paper-based data including Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII) information according to the NITC Incident Response Policy when the contractor or contractor’s employee first becomes aware of the loss or suspected loss. If the contractor or contractor’s employee does not have access to this procedure, then the incident should be immediately reported to the Agriculture Security Operations Center (ASOC) via the 24-hour Cyber Incidents Hotline, (866) 905-6890.

11.6. Permanent Security Badge Requirements

A permanent security badge will not be issued until the security questionnaire has been completed and favorably reviewed. In order to gain access to NITC authorized work locations via a permanent security badge, all contractor employees are required to complete the Request for USDA Identification (ID) Badge, Form Number AD-1197 (Sept 2005). The contract employee will be given this form upon first arrival for duty by the Contractor. Form Number AD-1197 (Sept. 2005) requires two (2) forms of identification be submitted. Contract employees are required to provide this identification when first reporting for work. One form of identification must any one of items 1-4 in the list below (Primary ID). The other ID may be any of the forms of ID listed below (Primary or Secondary ID types).

Acceptable Forms of ID:

Primary Forms of Identification (Items 1-4)	
1. US Passport (unexpired or expired)	3. US Military ID card (unexpired)

2. Driver's license or ID card issues by a state or possession of the United States provided it contains a photograph (unexpired)	4. US Military Dependent's ID Card (unexpired)
Secondary Forms of Identification (Items 5-25)	
5. US Social Security Card issued by the Social Security Administration	16. Permanent Resident Card or Alien Registration Receipt card with photograph (Form I-151 or I-1551)
6. Original or certified copy of a birth certificate issued by a state, county, municipal authority, or outlying possession of the United States bearing an official seal	17. Certification of Birth Abroad issued by the Department of State (Form FS-545 or Form DS-1350)
7. ID issued by federal, state, or local government agencies or entites, provided it contains a photograph.	18. Unexpired Temporary Resident Card (Form I-668)
8. School ID with photograph	19. Unexpired Employment Authorization Card (Form I-668A)
9. Voter's registration card	20. Unexpired Reentry Permit (Form I-327)
10. US Coast Guard Merchant Mariner card	21. Unexpired Refugee Travel Document (Form I-571)
11. Certificate of US Citizenship Form (Form N-560 or N-561)	22. Unexpired employment authorization document issued by DHS
12. Certificate of Naturalization (Form N-560 or N-570)	23. Unexpired Employment Authorization Document issued by DHS with photograph (Form I-668B)
13. US Citizen ID Card (Form 1-197)	24. Driver's license issued by a Canadian Government Authority
14. Unexpired foreign passport with I-551 stamp or attached Form I-94 indicating unexpired employment authorization	25. Native American tribal document
15. ID card for use of Resident Citizen in the United States (Form I-179)	

### *11.7.	Display of Permanent Security Badges*

A permanent security badge must be worn at all times while in the facility. It must be displayed above the waist. The individual will retain possession of the permanent security badge as long as continued admittance to the site is needed. Ensuring the safekeeping, wearing, and visibility of Government furnished security badge is the responsibility of the person issued a USDA Identification (ID) Badge. A permanent security badge shall immediately be returned to the Government when the need for it ceases to exist.

### *11.8.	Temporary Security Badge Requirements*

The Contractor shall ensure that each of the contractor's employees has been issued a temporary badge while the Request for USDA Identification (ID) Badge, Form Number AD-1197 (Sept 2005) is being proceeded. Temporary or visitor badges will be provided for persons who are identified as having an infrequent or temporary legitimate business need for access to the site. As noted above, tasks and task assignments that exceed 180 days will require a permanent badge. The temporary badge authorizes the wearer to enter and exit the secured areas where NITC workstations are located within applicable authorized work location. The badge must be worn at all times while in the facility. It must be displayed above the waist. The badge must be returned to the security desk at the close of the business day.

11.9. Facility Security Requirements

Due to NITC facility security policies, it is required that the facility guards be notified in advance of all visitors wanting to enter the facility. This 24-hour advanced notification must provide the names, dates, times, the nature of the visit and the visitor's point of contact (POC). All visitors must have a NITC POC in order to be admitted to the facility. Individuals arriving at the NITC data center facilities that do not provide a pre-arranged POC may be turned away.

- 8930 Ward Parkway Facility Visitors Entrance. The east lobby of the 8930 Ward Parkway facility is the entry point for all NITC visitors. Visitors shall check-in at the east lobby guard station, sign-in and be issued a visitor's badge. The visitor's POC will be notified of the visitor's arrival. The visitor will be screened by a hand-held magnetometer, and the visitor's belongings will be passed through an x-ray machine. Failure to voluntarily comply with these security measures will cause the visitor to be denied access to the facility. The visitor shall return all issued visitor's badges at the end of the day or upon leaving the facility for any reason. Point of Contact: PWS COR.

- St. Louis, Missouri Location at the Goodfellow Federal Center Complex. Entrance onto the Federal Center Complex is at the main gate accessible from Goodfellow Boulevard. The main gate is open 24/7 and manned by GSA security officers. All vehicles entering the Campus are required to have a permanent complex decal or a Federal Center Complex parking permit. This must be arranged with the point of contact before attempting to enter the Federal Center Complex. Visitors are required to undergo a vehicle inspection conducted by the guards at the gate. Visitors must sign in at the main entry and be on the entrance list prior to attempting to enter the Federal Center Complex. The visitor is issued a paper badge which is returned upon leaving the Complex. The visitor's point of contact (POC) is notified to come to the gate and escort the individual. The POC will coordinate the access requirements with the lead Agency, Rural Development. Point of Contact: Diego Maldonado, Diego.Maldonado@ocio.usda.gov.

- Washington, D.C. (NITC-DC) Location. The COR must sponsor all contract employees into the Whitten-South Building Complex. To process a contractor for a site identification badge, the federal sponsor must submit a form to, Tawana Waller, the headquarters security contact for all Office of the Chief Information Officer organizations. Once the proper background checks and security process determined to be adjudicated acceptably, the contractor would report to Room 1408-South (1st floor, 4th wing) for photo identification badging. Point of Contact: Bryan Dixon, Bryan.Dixon@ocio.usda.gov.

- George Washington Carver Center (GWCC), Beltsville, Maryland Location. The main entrance to the Carver Center is at Building 1. Building 1 has a 24x7 guard posted at the reception desk. Visitors check-in check at Building 1 reception desk, show a valid identification, sign-in and issued a visitor's badge and parking permit. The visitor's belongings are than passed through an x-ray machine. The visitor's POC will be notified of their arrival and escorted within the facility. Badging office is located in Building 1 just east of the reception desk. Point of Contact: Bryan Dixon, Bryan.Dixon@ocio.usda.gov.

- Salt Lake City, Utah Location. The facility is open from 6am-6pm/Mountain time, Monday-Friday (closed Federal holidays). The facility is open to the general public. The public entry point is at the East side of the facility next to the flagpole. All general public are required to sign in, issued a temporary day-use visitor pass. Visitors needing access beyond the Customer Service Area need to be escorted by the POC. The visitor's POC will be notified of their arrival and escorted within the facility. Point of Contact: Lori Uhlhorn, lori.uhlhorn@slc.usda.gov; Denny Skiles, denny.skiles@slc.usda.gov.

- Ft. Worth, Texas Location at the National Geospatial Center of Excellence with the Fort Worth Federal Center. The Fort Worth Federal Center entrance is at the main gate at 501 W. Felix Street. Boulevard.

The main gate is open 24/7 and manned by GSA security officers. Visitors are required to undergo a vehicle inspection conducted by the guards at the gate. The visitor's point of contact (POC) should be notified 24 hours in advance. The visitor's POC will be notified to come to the gate and escort the individual. The POC will coordinate the access requirements to Building 23 or 24, as applicable. Point of Contact: Paul Fukuhara, paul.fukuhara@ftw.usda.gov

- Ft. Collins, Colorado location at the Forest Services' Natural Resources Research Center, Building A, on the Colorado State University campus. The Natural Resources Research Center (NRRC) is located at 2150 Centre Avenue, Building A, Fort Collins, CO 80526. The main entrance is during normal business hours to visitors. The visitor's point of contact (POC) should be notified 24 hours in advance. The visitor's POC will be notified to come to the entrance and escort the individual. The POC will coordinate the access requirements to the building, as applicable. Point of Contact: Rick Rohlfs, rick.rohlfs@ocio.usda.gov; Jordan Bancroft, (970-295-5710).

11.10. Parking Requirements

The contractor shall direct its employees to comply with applicable rules governing parking at each authorized work location. These rules may include the display of a parking permit in the windshield of a vehicle or the application of a parking permit to the exterior of a vehicle.

- 8930 Ward Parkway Facility Parking Requirements: The Contractor shall ensure that each contractor employee obtains a parking permit tag from the Government Security Staff. The tag shall be properly displayed and visible on any vehicle parked near the 8930 Ward Parkway physical plant. Vehicles only intermittently visiting the 8930 Ward Parkway facility shall park in the visitor parking area.
- St. Louis, Missouri Location at the Goodfellow Federal Complex: All vehicles on the Federal Center Complex grounds must have a permanent window decal or a Federal Center parking permit. Contact the St. Louis facility POC for arranging the appropriate vehicle pass.
- Washington, D.C. (NITC-DC) Location: There is no government provided parking available at this location.
- George Washington Carver Center (GWCC), Beltsville, Maryland Location: There is a separate parking area designated for visitors. USDA and contract employees from other locations are required to check in at the reception desk and get a temporary parking permit and park in employee parking area. Contact the GWCC POC for arranging the appropriate vehicle pass.
- Salt Lake City, Utah Location: The main parking lot is located East of the building with smaller lots located North and South of the main building. Contact the Salt Lake City for arranging the appropriate vehicle pass.
- Ft. Worth, Texas Location: From the guardhouse, proceed downhill, across the railroad tracks and take the second right. As you turn right you will go under Hemphill Street. Follow the street as it curves to the left. Yield at the sign, then cross the street into the parking lot on the east side of Building 23. Visitor parking is designated. Enter the building through the automatic doors under the blue awning. Contact the Fort Worth POC to arrange for a permanent vehicle pass.
- Ft. Collins, Colorado location: There are separate designated parking spaces for visitors. A temporary parking permit must be displayed on the dashboard of visitor vehicles. The temporary parking permit will be provided by the guard in Building A. Contact the Ft. Collins POC to arrange for a permanent vehicle pass.

12. ADMINISTRATIVE CONSIDERATIONS

12.1. Government Representatives

GSA Contracting Officer's Representative
Wendi Borrenpohl
1710 Corporate Crossing, Ste. 3
O'Fallon, IL 62269
(b) (6)
wendi.borrenpohl@gsa.gov

GSA Contracting Officer
Yjuania Still
1710 Corporate Crossing, Ste. 3
O'Fallon, IL 62269
(b) (6)
yjuania.still@gsa.gov

Client Contracting Officer's Representative
Carrie Coffman
USDA, NITC, Resource Management Division (RMD)-RSSB
8930 Ward Parkway
Kansas City, MO 64114
(b) (6)
carrie.coffman@ocio.usda.gov

12.2. Procedures for Payment

12.2.1. Performance Based Payment Percentages

The performance objectives and respective payment percentages based on relative importance to total task performance are identified in the CLIN descriptions contained in PWS Attachment A. This document also identifies the Government's proposed surveillance assurance methodology.

12.2.2. Submission

Invoices are due no later than the 15th calendar day of the month following the reporting period. The contractor shall submit the invoices and supporting documents, through ITSS simultaneously with the MSR (as an acceptance item) to allow the client and the COR to electronically accept and certify services received by the client representative. The contractor is authorized to invoice only for the services and travel ordered by GSA and provided in direct support of the task order.

12.2.3. Non-Compliance

Failure to comply with the procedures outlined may result in payment being delayed at no additional cost to the Government.

12.3. Personal Service

The client determined that use of the GSA requirements contract to satisfy this requirement is in the best interest of the Government, economic and other factors considered, and this task order is not being used to procure personal services prohibited by the Federal Acquisition Regulation (FAR) Part 37.104 titled "Personal Services Contract". The Contractor agrees that this is a non-personal services task order. The Contractor is not, nor shall it hold itself out, to be an agent or partner of, or joint venture with, the Government. The Contractor agrees that his/her personnel shall neither supervise nor accept supervision from Government employees.

12.4. Section 508

All services and products provided in response to the requirements identified in this document shall comply with Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), and the Architectural and Transportation Barriers Compliance Board Electronic and IT (EIT) Accessibility Standards (36 CFR part 1194).

12.5. Privacy Act

Work under this task order requires that personnel have access to Privacy Information. Contractor personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable USDA rules and regulations.

ID05140054 Performance Standards and Acceptable Quality Levels for all Labor Hour Contract Line Item Numbers (CLINs) (CLIN 013 through CLIN 029)

Support Item / Area	Performance Standard	Acceptable Quality Level (AQL)
Availability	■ 100% contractor personnel availability during required daily core hours or specific CLIN required schedules (with the exception of coordinated absences). ■ The contractor is responsible for resource substitution/coverage when a coordinated absence is greater than five consecutive work days.	No more than the identified violations as bulletted immediately below, per month. - CLINs with 1 to 5 individual task order performers providing support shall have no more than 4 violations. - CLINs with 6 to 10 individual task order performers providing support shall have no more than 6 violations. - CLINs with 11 to 15 individual task order performers providing support shall have no more than 8 violations. - CLINs with 16 to 20 individual task order performers providing support shall have no more than 10 violations. - CLINs with 21 to 30 individual task order performers providing support shall have no more than 12 violations. - CLINs with 30 to 40 individual task order performers providing support shall have no more than 14 violations. - The Government reserves the right to incorporate additional AQLs as needed consistent with those identified. No more than 50% of the monthly violations shall be performed by an individual task order performer for CLINs that are supported by five or more individual task order performers. Each violation may be reflected as such within the CPARS assessment.
Work/Task Product Activities	■ All operational support activities shall be conducted in accordance with governmental & organizational standards, policies, directives, standard operating procedures, work instructions, processes & guidance. All operational support activities shall be captured and properly documented in the organizational ITSM tool. The contractor shall adhere to this requirement unless a written exemption is issued by an authorized Government representative.	No more than the identified violations as bulletted immediately below, per month. - CLINs with 1 to 5 individual task order performers providing support shall have no more than 4 violations. - CLINs with 6 to 10 individual task order performers providing support shall have no more than 6 violations. - CLINs with 11 to 15 individual task order performers providing support shall have no more than 8 violations. - CLINs with 16 to 20 individual task order performers providing support shall have no more than 10 violations. - CLINs with 21 to 30 individual task order performers providing support shall have no more than 12 violations. - CLINs with 30 to 40 individual task order performers providing support shall have no more than 14 violations. - The Government reserves the right to incorporate additional AQLs as needed consistent with those identified. No more than 50% of the monthly violations shall be performed by an individual task order performer for CLINs that are supported by five or more individual task order performers. In addition to violations for non-compliance with the specific performance standards identified in cell B5 , errors (including grammatical errors), omissions, and delayed deliveries are considered violations. Each violation may be reflected as such within the CPARS assessment.
Security Incident Notification and Resolution	■ 100% of security incidents, Personally Identifyable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660). ■ 100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be addressed in accordance with Government direction.	No allowable violations per month for any CLIN. In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring. Each violation may be reflected as such within the CPARS assessment.

FFP - Transition Period

Task Order CLIN (if applicable)	ASB CLIN	CLIN Type	ASB Labor Category Title	Task Order CLIN and/or Transition Period Position Title	Hours	Ceiling Rate	Percentage Discount	Discounted Rate	Total
		FFP	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
FFP TOTAL									$0.00

Task Order CLIN	ASB CLIN	CLIN Type	ASB Labor Category Title	Task Order CLIN Title	Hours	Ceiling Rate	Percentage Discount	Discounted Rate	Total
001		FFP	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
002		FFP	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
003		FFP	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
004		FFP	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
005		FFP	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
006		FFP	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
007		FFP	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
008		FFP	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
009		FFP	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
010		FFP	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
011		FFP	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
012		FFP	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
FFP CORE TOTAL					0.00				$0.00
FFP GROWTH TOTAL (predetermined 78% growth calculation)									$0.00
FFP TOTAL									$0.00

Task Order CLIN	ASB CLIN	CLIN Type	ASB Labor Category Title	Task Order CLIN Title	Hours	Ceiling Rate	Percentage Discount	Discounted Rate	Total
013		LH	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
014		LH	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
015		LH	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
016		LH	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
017		LH	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
018		LH	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
019		LH	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
020		LH	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
021		LH	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
022		LH	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
023		LH	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
024		LH	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
025		LH	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
026		LH	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
027		LH	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
028		LH	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
029		LH	insert a separate line for each proposed position	insert a separate line for each proposed position	0.00	$100.00	10.00%	$90.00	$0.00
SUB-TOTAL					0.00				$0.00
LH CORE TOTAL					0.00				0.00
LH GROWTH TOTAL (predetermined 56% growth calculation)									$0.00
LH TOTAL									$0.00

CLIN	Transition Period	Base Period	Option Period #1	Option Period #2	Option Period #3
001	[redacted]	$0.00	$0.00	$0.00	$0.00
002	[redacted]	$0.00	$0.00	$0.00	$0.00
003	(b) (4) [redacted]	$0.00	$0.00	$0.00	$0.00
004	[redacted]	$0.00	$0.00	$0.00	$0.00
005	[redacted]	$0.00	$0.00	$0.00	$0.00
006	[redacted]	$0.00	$0.00	$0.00	$0.00
007	[redacted]	$0.00	$0.00	$0.00	$0.00
008	[redacted]	$0.00	$0.00	$0.00	$0.00
009	[redacted]	$0.00	$0.00	$0.00	$0.00
010	[redacted]	$0.00	$0.00	$0.00	$0.00
011	[redacted]	$0.00	$0.00	$0.00	$0.00
012	[redacted]	$0.00	$0.00	$0.00	$0.00
013	[redacted]	$0.00	$0.00	$0.00	$0.00
014	[redacted]	$0.00	$0.00	$0.00	$0.00
015	[redacted]	$0.00	$0.00	$0.00	$0.00
016	[redacted]	$0.00	$0.00	$0.00	$0.00
017	[redacted]	$0.00	$0.00	$0.00	$0.00
018	[redacted]	$0.00	$0.00	$0.00	$0.00
019	[redacted]	$0.00	$0.00	$0.00	$0.00
020	[redacted]	$0.00	$0.00	$0.00	$0.00
021	[redacted]	$0.00	$0.00	$0.00	$0.00
022	[redacted]	$0.00	$0.00	$0.00	$0.00
023	[redacted]	$0.00	$0.00	$0.00	$0.00
024	[redacted]	$0.00	$0.00	$0.00	$0.00
025	[redacted]	$0.00	$0.00	$0.00	$0.00
026	[redacted]	$0.00	$0.00	$0.00	$0.00
027	[redacted]	$0.00	$0.00	$0.00	$0.00
028	[redacted]	$0.00	$0.00	$0.00	$0.00
029	[redacted]	$0.00	$0.00	$0.00	$0.00
Subtotal FFP Labor - Core	$0.00	$0.00	$0.00	$0.00	$0.00
Subtotal LH Labor - Core	$0.00	$0.00	$0.00	$0.00	$0.00
Subtotal Labor - Core	$0.00	$0.00	$0.00	$0.00	$0.00
CAF	$0.00	$100,000.00	$100,000.00	$100,000.00	$100,000.00
Travel	$0.00	$10,000.00	$10,000.00	$10,000.00	$10,000.00
Subtotal - Core	$0.00	$110,000.00	$110,000.00	$110,000.00	$110,000.00
(b) (4) [redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Subtotal FFP - Growth	$0.00	$0.00	$0.00	$0.00	$0.00
Subtotal LH - Growth	$0.00	$0.00	$0.00	$0.00	$0.00
Subtotal - Growth	$0.00	$0.00	$0.00	$0.00	$0.00
(b) (4) [redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
otal FFP Labor	$0.00	$0.00	$0.00	$0.00	$0.00
Subtotal LH Labor	$0.00	$0.00	$0.00	$0.00	$0.00
(b) (4) [redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Total	$0.00	$110,000.00	$110,000.00	$110,000.00	$110,000.00

Option Period #4	Total
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$100,000.00	$500,000.00
$10,000.00	$50,000.00
$110,000.00	$550,000.00
(b) (4)	
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
(b) (4)	
$0.00	$0.00
$0.00	$0.00
(b) (4)	
$110,000.00	$550,000.00

ASB Labor Category	Base Period Ceiling Rate	Base Period Discount Percentage	Base Period Discounted Rate
Administration/Clerical	[redacted]	[redacted]	[redacted] (b) (4)
Administration/Clerical (Entry Level)			$0.00
Administration/Clerical (Journeyman)			$0.00
Administration/Clerical (Senior)			$0.00
Applications Developer	[redacted]	[redacted]	[redacted] (b) (4)
Applications Developer (Entry Level)			$0.00
Applications Developer (Journeyman)			$0.00
Applications Developer (Senior)			$0.00
Applications Developer (Master)			$0.00
Applications Systems Analyst	[redacted]	[redacted]	[redacted] (b) (4)
Applications Systems Analyst (Entry Level)			$0.00
Applications Systems Analyst (Journeyman)			$0.00
Applications Systems Analyst (Senior)			$0.00
Applications Systems Analyst (Master)			$0.00
Business Process Consultant			$0.00
Business Systems Analyst			$0.00
Chief Information Security Officer			$0.00
Computer Scientist			$0.00
Computer Forensic and Intrusion Analyst			$0.00
Configuration Management Specialist	[redacted]	[redacted]	[redacted] (b) (4)
Configuration Management Specialist (Journeyman)			$0.00
Configuration Management Specialist (Senior)			$0.00
Configuration Management Specialist (Master)			$0.00
Data Architect			$0.00
Data Warehousing Specialist	[redacted]	[redacted]	[redacted] (b) (4)
Data Warehousing Specialist (Entry Level)			$0.00
Data Warehousing Specialist (Journeyman)			$0.00
Data Warehousing Specialist (Senior)			$0.00
Data Warehousing Specialist (Master)			$0.00
Database Specialist	[redacted]	[redacted]	[redacted] (b) (4)
Database Specialist (Entry Level)			$0.00
Database Specialist (Journeyman)			$0.00
Database Specialist (Senior)			$0.00
Database Specialist (Master)			$0.00
Disaster Recovery Specialist	[redacted]	[redacted]	[redacted] (b) (4)
Disaster Recovery Specialist (Journeyman)			$0.00
Disaster Recovery Specialist (Senior)			$0.00
Enterprise Architect			$0.00
ERP Analyst			$0.00
ERP Business/Architectural Specialist			$0.00
Financial Analyst			$0.00
GIS Analyst/Programmer			$0.00
Graphics Specialist			$0.00
Groupware Specialist			$0.00
Hardware Engineer	[redacted]	[redacted]	[redacted] (b) (4)
Hardware Engineer (Entry Level)			$0.00
Hardware Engineer (Journeyman)			$0.00
Hardware Engineer (Senior)			$0.00
Hardware Engineer (Master)			$0.00
Helpdesk Specialist	[redacted]	[redacted]	[redacted] (b) (4)
Helpdesk Specialist (Entry Level)			

Helpdesk Specialist (Journeyman)			$0.00
Helpdesk Specialist (Senior)			$0.00
Information Assurance/Security Specialist	[redacted]	[redacted]	[redacted] (b) (4)
Information Assurance/Security Specialist (Entry Level)			$0.00
Information Assurance/Security Specialist (Journeyman)			$0.00
Information Assurance/Security Specialist (Senior)			$0.00
Information Assurance/Security Specialist (Master)			$0.00
Information Specialist/Knowledge Engineer			$0.00
Modeling and Simulation Specialist			$0.00
Network Specialist	[redacted]	[redacted]	[redacted] (b) (4)
Network Specialist (Entry Level)			$0.00
Network Specialist (Journeyman)			$0.00
Network Specialist (Senior)			$0.00
Network Specialist (Master)			$0.00
Program Manager			$0.00
Project Manager			$0.00
Quality Assurance Specialist	[redacted]	[redacted]	[redacted] (b) (4)
Quality Assurance Specialist (Entry Level)			$0.00
Quality Assurance Specialist (Journeyman)			$0.00
Quality Assurance Specialist (Senior)			$0.00
Quality Assurance Specialist (Master)			$0.00
Research Analyst			$0.00
Strategic/Capital Planner			$0.00
Subject Matter Expert	[redacted]	[redacted]	[redacted] (b) (4)
Subject Matter Expert (Journeyman)	[redacted]	[redacted]	[redacted]
Subject Matter Expert (Senior)			$0.00
Subject Matter Expert (Master)			$0.00
Systems Engineer			$0.00
Technical Editor			$0.00
Technical Writer			$0.00
Test Engineer	[redacted]	[redacted]	[redacted] (b) (4)
Test Engineer (Entry Level)			$0.00
Test Engineer (Journeyman)			$0.00
Test Engineer (Senior)			$0.00
Training Specialist	[redacted]	[redacted]	[redacted] (b) (4)
Training Specialist (Entry Level)			$0.00
Training Specialist (Journeyman)			$0.00
Training Specialist (Senior)			$0.00
Voice/Data Communications Engineer	[redacted]	[redacted]	[redacted] (b) (4)
Voice/Data Communications Engineer (Entry Level)			$0.00
Voice/Data Communications Engineer (Journeyman)			$0.00
Voice/Data Communications Engineer (Senior)			$0.00
Voice/Data Communications Engineer (Master)			$0.00
Web Content Analyst			$0.00
Web Designer			$0.00

Option Period #1 Rate	Option Period #1 Discount Percentage	Option Period #1 Discounted Rate	Option Period #2 Rate	Option Period #2 Discount Percentage	Option Period #2 Discounted Rate	Option Period #3 Rate	Option Period #3 Discount Percentage
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted] (b) (4)
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted] (b) (4)
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted] (b) (4)
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted] (b) (4)
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted] (b) (4)
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted] (b) (4)
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted] (b) (4)
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted] (b) (4)
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted] (b) (4)
		$0.00			$0.00		

		$0.00			$0.00		
		$0.00			$0.00		
[redacted]							(b) (4)
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
[redacted]							(b) (4)
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
[redacted]							(b) (4)
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
[redacted]							(b) (4)
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
[redacted]							(b) (4)
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
[redacted]							(b) (4)
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
[redacted]							(b) (4)
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		
		$0.00			$0.00		

Option Period #3 Discounted Rate	Option Period #4 Rate	Option Period #4 Discount Percentage	Option Period #4 Discounted Rate
			(b) (4)
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
			(b) (4)
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
			(b) (4)
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
			(b) (4)
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
			(b) (4)
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
			(b) (4)
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
			(b) (4)
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
			(b) (4)
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
			(b) (4)
$0.00			$0.00

$0.00			$0.00
$0.00			$0.00
(b) (4)			
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
(b) (4)			
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
(b) (4)			
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
(b) (4)			
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
(b) (4)			
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
(b) (4)			
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
(b) (4)			
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00
$0.00			$0.00

GSA RFQ949010 (GSA Task Id ID05140054)
Amendment #5

Clarification Document dated 2015.02.03

The purpose of this clarification document is to address questions submitted in response to the Request for Proposal (RFP), amendment #4. The questions have not been altered. The clarification document will be incorporated into the resultant task order award. Furthermore, the release of the subject clarification incorporates the items listed below into the RFP. The revisions hereby replace previous versions of the same documents in their entirety.

RFP 2015.02.03 – revision 2

No additional questions will be considered.

1. Reference: The revised RFP released on 1/23 states "Furthermore, the ASB prime contractor is required to include (within the three references identified above) at least one project supporting a Federal Agency that the ASB prime contractor performed ~~and completed~~ as the prime with an annual value, for each annual period of performance included within the project, of no less than $2 million. " Also reference clarification document question 183. Question 1: The removal of the lined out wording "and completed" appears to allow performance periods which were awarded at 2M per year or above, but, which have not yet been performed, to qualify the reference. Is that correct?

   ***Answer:* The removal of the word "completed" allows contractors to include current, on-going references/projects within the past performance submission; however, the Government reserves the right to give additional weight to completed past performance references/projects in the evaluation process.**

2. Reference: Clarification Reference Q&A # 151 "Answer: Confirmation denied. The minimum value for each annual period of performance included within the reference shall be no less than $2 million. " Question 2: Not all periods of performance are 1 year. If the initial period of performance for the past performance reference is completed prior to proposal due date, but was less than one year in length, can the yearly equivalent of that period or performance satisfy the 2M per year performance level required?

   ***Answer:* No. The past performance reference shall be of a sufficient duration to satisfy the stated requirements.**

3. Can the cover/title page providing identifying information of contractor, volume, and proprietary markings be outside of the page count?

   ***Answer:* No; however, the standalone file containing the cover letter (reference Request for Proposal (RFP) paragraph [(III)(A)(3)] is excluded from the page limitation.**

4. Clarification, page 17 of 34, answer 90, states that "Tab separators with no written content are not included within the established page limitation." Are tabs with section titles (e.g., Appendix A, Section X –Staffing) on them excluded from the page limitation?

   ***Answer:* Tab separators with no written content, other than section identification, are not included within the established page limitation.**

5. Clarification, page 28, answer to question number 153, requires that subcontractors provide contract or purchase order under which either a cure notice or show cause letter was received, or any contract or purchase order that was terminated for cause by the Government within the past three years." Given that this information is proprietary, can the subcontractor submit its response to this requirement directly to the CO via email and send in a sealed envelope with the hard copies to satisfy the requirement under 3 (c) and the submission requirements? If so, please confirm that this separate response will not be included in the overall page count.

Answer: ***Confirmed. The separate response is excluded from the established page limitation; however, the subject response, in its entirety, is limited to five pages.***

6. RFP, page 12, IX. States, "Electronic proposals must be submitted no later than the date established in the eBuy, with six hardcopies to be delivered no later than the first business day of this date/time, to:…"

   a) Was this intended to say, "delivered no later than the first business day after this date/time"?

      Answer: ***The language was written as intended. Furthermore, the language shall be interpreted as no later than the first business day after the closure date established in the eBuy system.***

   b) Confirm that the hardcopy delivery date is February 23, 2015.

      Answer: ***Confirmed.***

   c) By what time/hour must hard copies be delivered?

      Answer: ***4:00 PM Central Standard Time (CST).***

7. RFP, page 12, "Due Date" says, "…with six hardcopies to be delivered within 24 hours of this date/time…"? This is the only instruction regarding hardcopy delivery.

   Answer: ***Refer to the response to question #6.***

   a) Are binders acceptable for submitting hardcopies?

      Answer: ***Yes.***

   b) If binders are acceptable, will the cover page of the binders be excluded from page count?

      Answer: ***No; however, the identification page inserted within the plastic on the outside of the binder is not included within the established page limitation.***

8. In RFP paragraph IV.B.1.b, the Government states, "The prime contractor shall also provide information on any subcontractor proposed."? The prime is required to provide the ASB number, address, contract administration POC, technical POC, and business size. Is the same information required for subcontractors?

   Answer: ***Refer to the response to question #7 in the Clarification Document dated January 23, 2015 (released via RFP amendment #4).***

9. Attachment 1, 9.5, Hours of Work. Is the calculation of the monthly allocation of hours by individual employee, CLIN, or total contract level

   Answer: ***The referenced calculation is based on a full-time equivalent position.***

REQUEST FOR PROPOSAL
ID05140054

In Support Of

CLIENT AGENCY:

United States Department of Agriculture (USDA)
National Information Technology Center (NITC)

PROJECT TITLE:
Information Technology Support

~~**Original Version dated December 18, 2014**~~

~~**Revision 1 dated January 23, 2015**~~

Revision 2 dated February 3, 2015

Table of Contents

I. INTRODUCTION 3

A. Performance Based Contracting Approach 3

B. Period of Performance 3

C. Level of Support 3

II. MINIMUM REQUIREMENTS - READ THIS FIRST 3

III. INSTRUCTIONS TO CONTRACTORS 4

A. Submission of Proposal 4

B. General Contractor Instructions 4

IV. PROPOSAL CONTENT 5

A. General 5

B. Detailed 5

1. Cover Letter 5
2. Technical Capability 6
3. Past Experience and Performance 8
4. Price Submission 9

V. EVALUATION CRITERIA AND SELECTION PROCESS 9

A. General 9

B. Evaluation Factors 10

1. FACTOR 1: Technical Capability 10
2. FACTOR 2: Past Experience and Performance 10
3. FACTOR 3: Price 10

VI. SELECTION 10

A. Best Value Evaluation 10

B. Discussions and Competitive Range. 10

VII. ADDITIONAL TERMS AND CONDITIONS 11

VIII.RFP QUESTIONS 12

IX. DUE DATE 13

DATE: February 3, 2015

MEMORANDUM FOR: General Services Administration (GSA)
Alliant Small Business (ASB)
Governmentwide Acquisition Contract (GWAC)

FROM: GSA
Federal Acquisition Service (FAS)
Acquisition Operations Division (5QZA)
1710 Corporate Crossing, Ste. #3
O'Fallon, IL 62269

SUBJECT: Request for Proposal (RFP) for GSA Order Number ID05140054

I. INTRODUCTION

It is the intent of the GSA FAS 5QZA to issue a single-award task order against the GSA ASB GWAC to provide a full range of Information Technology (IT) services in support of the United States Department of Agriculture (USDA), National Information Technology Center (NITC).

A. *Performance Based Contracting Approach*

This RFP utilizes a Performance Work Statement (PWS) (**RFP Attachment 1**) to provide the Government's overall desired outcomes/objectives for this requirement. The PWS provides the overall scope and general requirements. Specific task requirements are identified in **PWS Attachment A** via the utilization of Contract Line Item Number (CLIN) descriptions. The performance standards and acceptable quality levels are identified in both PWS Attachment A and **PWS Attachment B**, Labor Hour CLIN Service Delivery Summary, as applicable.

B. *Period of Performance*

The resulting task order will have a one-year base period and four, one-year option periods.

C. *Level of Support*

For indicating the scope of work only, the estimated core initial staffing levels in terms of Full-Time-Equivalent (FTE) positions are identified in **PWS Attachment C**. It is anticipated that the workload will fluctuate based on fluid schedule requirements; therefore, the contractor shall include provisions for optional growth support throughout the task order life cycle as reflected in the pricing template, which includes lump sum labor allotments for optional growth support that are equivalent to a percentage of the price/cost for the core requirements. To ensure maximum flexibility with respect to the optional growth support, the contractor shall include a complete price list identifying the proposed hourly labor rates for all ASB labor categories (LCATs), as reflected in the pricing template, that will be used as the pricing basis for all optional growth support. The actual time frame for the optional growth support implementation will be dependent upon actual scheduling requirements.

II. MINIMUM REQUIREMENTS - READ THIS FIRST

Contractor proposals submitted in response to this RFP must comply with the following minimum requirements. Proposals that fail to meet any ONE of these minimum requirements may be eliminated from further consideration and deemed ineligible for award.

- Submit complete information as required in these instructions.
- Comply with all requirements identified in these instructions.

- As detailed in section III, all electronic documents/data submitted must be enabled so that the text/data in those documents/data can be searched, highlighted, copied and pasted into other documents/spreadsheets as needed.
- The contractor shall utilize and fully complete the required pricing template (**RFP Attachment 2**). Contractor proposed labor rates shall not exceed the applicable contract ceiling rates.
- The contractor shall complete the registration process (contractor company, contractor company representatives, and ASB contract) for GSA's web-based procurement system, Information Technology Solutions Shop (ITSS). Contractors may contact the ITSS Registration Helpdesk at 877-243-2889, option #2, for registration assistance.

III. INSTRUCTIONS TO CONTRACTORS

A. *Submission of Proposal*

1. Proposals shall be received no later than the date identified in paragraph IX. Proposals received after this time will not be considered for award. All proposals shall be uploaded to eBuy (www.ebuy.gsa.gov) under the applicable RFP. Regarding page limitations, the documentation shall be single-spaced, Times New Roman font (no exceptions), no smaller than 11 point type-size, no less than 1 inch margins, that (if printed) would fit on 8 ½ x 11 inch paper. The only exception to the paper size (not an exception to the font requirements) is for the price proposal and the organizational chart. The price proposal shall be printed on paper of a sufficient size to allow each sheet within the pricing template to be printed on a single page. The organizational chart shall be printed on paper of sufficient size to allow the entire chart to be displayed on a single page.

2. The acceptable electronic formats are Adobe PDF or Microsoft Word except for pricing. Price proposals shall be submitted using the required pricing template. All Adobe PDF documents and Microsoft Word documents shall be submitted with the ability to highlight and copy the text/data of the document. Any documents submitted that are protected in such a way which does not enable the ability to highlight/copy/paste the text/data will not be accepted. All Microsoft Word documents shall be fully readable by Microsoft Office version 2007.

3. Pricing proposal information shall not contain any technical proposal information and vice versa. When uploading the proposal to eBuy, separate all pricing and technical proposal information into separate zip (winszip.exe) folders. The naming convention for the WinZip folders shall be as follows: for pricing "GS-06F-XXXXX PRICING.zip", for Technical "GS-06F-XXXXX TECH.zip" (Complete the X's with the GSA ASB contract number). Submit the cover letter as a standalone document with the same style of naming convention "GS-06F-XXXXX COVER LETTER." All past performance information shall be included within the "GS-06F-XXXXX TECH.zip" file.

4. As stated in Section IX, hard copies are also requested. Timeliness and responsiveness of the proposasl is first determined by the submission of the electronic proposal in eBuy, then followed by the delivery of the hard-copy proposals. Hard copy proposals are to be delivered to the address listed in paragraph IX no later than 24 hours following the close date/time identified in the same paragraph. Failure to meet both the eBuy submission and hard-copy submission deadlines will remove the proposal from consideration. The electronic submission will serve as the "official" submission.

B. *General Contractor Instructions*

1. Proposals shall clearly demonstrate an understanding of each of the Government's objectives and requirements.

2. A complete proposal shall consist of a cover letter; a technical proposal, including both a technical capability section and a past experience and performance section; and a price proposal as detailed below. Incomplete proposals will not be further evaluated and deemed ineligible for award.

3. Proposals submitted in any other way except as detailed in the submission of proposals section above will not be further evaluated and deemed ineligible for award.

4. Any proposal or proposal modification will not be accepted after the due date and time for proposals.

5. Any assumptions forming the basis of the proposal, whether technical or price related, must be clearly identified in the applicable proposal.

6. All proposals shall be handled in accordance with FAR Subpart 3.104, Procurement Integrity.

7. Information requested herein must be furnished in writing and be fully and completely in compliance with RFP instructions. The information requested and the manner of submission is essential to permit prompt evaluation of all proposals on a fair and uniform basis. Simple statements of compliance without the detailed description of how compliance will be accomplished may not be considered sufficient evidence that the contractor can meet the technical requirements.

8. Contractor employees responsible for preparing material that may be procurement sensitive/proprietary data must mark each page that the contractor believes contains such information with the legend "Proprietary Data".

IV. PROPOSAL CONTENT

A. *General*

1. Contractors should review the GSA ASB contract and are responsible for ensuring that proposals fully comply with all GSA ASB contract requirements. Each proposal shall clearly demonstrate that the contractor understands the PWS. The failure to explain the contractor's ability to meet all requirements may result in the contractor's proposal not being considered. Clarity and completeness of proposals are of the utmost importance. Therefore, proposals must be written in a practical, clear and concise manner.

2. The narrative shall provide the Government with a reasonable assurance that the contractor has the relevant experience, capacity and capability required to meet or exceed the requirements and Government objectives identified within the PWS. A mere restatement of the PWS will be deemed unacceptable and may result in the contractor being eliminated from further consideration and deemed ineligible for award.

3. Each proposal shall be legible, single-spaced, typewritten Times New Roman font (no exceptions), no smaller than 11 point type-size, no less than 1 inch margins, which can be printed on 8 ½ x 11 inch paper (with the exception of the price proposal and organizational chart as per paragraph (III)(A)(1)). Overall proposal content, excluding the pricing submission, complete labor category skill level descriptions, and stand-alone cover letter, shall be no more than 45 pages in length.

B. *Detailed*

1. Cover Letter - An authorized official who can obligate the contractor shall sign a Cover Letter in contractor format, on contractor letterhead, demonstrating the contractor's intent to be bound to the task order terms and conditions. This cover letter shall be no more than two (2) pages. The cover letter shall include:

   a) Alliant Small Business Contractor Company Name, Address, Contract Administration POC name/phone/email, Technical POC name/phone/email (if different than Contract Administration POC), CAGE, DUNS, TIN, Business Size, and GSA ASB Number.

   b) Subcontractor Information: The prime contractor shall also provide information on any subcontractor proposed. The cover letter shall identify and describe, in sufficient detail, any

proposed/potential sub-contractor agreements that may be required in the performance and completion of the task requirements.

2. Technical Capability (part of the technical proposal) - The written technical capability section of the technical proposal shall contain the following:

   a) Technical Approach

      i. Understanding and Methodology. The technical proposal shall include an overview of the methodology that will be utilized to guide the management and performance of the technical requirements identified in the PWS. The proposal shall include sufficient documentation to demonstrate both a detailed understanding of the stated requirements and the potential management challenges associated with the broad range of task areas involved. The technical proposal shall include a description of how the technical approach (i.e. description of the tasks to be performed) and analytical techniques will be applied to accomplish each of the requirements identified in the PWS.
      ii. Implementation. The technical approach shall include a phase-in plan to address the overall transition to the new task order, to include the recruitment and hiring of both new and incumbent contractor employees, and include sufficient documentation to demonstrate that the USDA will not experience a negative impact or disruption in service as a result from contractor personnel changes. The proposal shall identify all Government coordination that is anticipated to be required for the implementation. Detailed requirements for the phase-in plan are identified in PWS paragraph 8.7.1. If applicable, the phase-in plan shall clearly describe the contractor's proposed transition period, as defined in PWS paragraph 8.7.1., to include the following: specific duration of the transition period; detailed description of the proposed tasks to be completed during the transition period; and the identification of the resources proposed to complete such tasks during the transition period.

   b) Quality Control Plan (QCP). The plan shall include, but is not limited to the following:

      i. A description of the inspection system covering all services listed.
      ii. The inspection frequency.
      iii. The title of the individual(s) who shall perform the inspection and their organizational placement.
      iv. A description of the methods for identifying, correcting, and preventing defects in the quality of service performed before the level becomes unacceptable.

   c) Staffing Approach/Plan. The proposal shall include a complete staffing approach/plan that describes and illustrates the proposed utilization of contractor personnel resources and skill sets to perform and complete the PWS requirements. The staffing approach/plan shall include, at a minimum:

      i. An organization chart that depicts the complete staffing approach/plan and structure from the <u>head of the company to all individual performers/positions</u> (including key positions and non-key positions) proposed to support the resultant task order that demonstrates required personnel resources and skill sets via the identification of proposed labor categories for all individual performers/positions. The organization chart shall include the following:
         - A clear illustration of the operational relationships and task leadership among all entities, including all proposed joint venture team members and subcontractors, and the alignment of such entities. NOTE: The proposal shall include a narrative discussion identifying the roles and responsibilities of all proposed joint venture team members and subcontractors.
         - The identification of all proposed positions, to include the identification of all positions as either "key" or "non-key".

- The names of known individuals proposed to perform and fill positions. Positions to be filled by future identified proposed staffing shall be reflected by the use of "TBD" in lieu of a proper name.
- The United States (U.S.) citizenship status, if known, of all known individuals proposed to perform and fill positions. Positions to be filled by future identified proposed staffing shall also include such identification to illustrate the contractor's intent. In addition, the chart shall include the identification of the overall percentage, in numerical format, of proposed U.S. citizens and non-U.S. citizens.
- The name of the contractor company that will employ the individuals that staff all proposed positions.
- The identification of the physical locations for all proposed positions depicted on the chart.
- The identification of the proposed ASB labor category (LCAT) and PWS CLIN for all proposed positions.

ii. Resumes of proposed staffing for all key positions, which identify the education, certification, experience, background investigation status, and special skills of any individual(s) proposed to fill these positions as required by the applicable ASB LCAT. The resumes shall also include the identification of the experience, certifications, and expertise identified in the PWS as applicable and available. All resumes included within the proposal submission shall identify the proposed LCAT from the ASB contract and the PWS CLIN that the staffing member is being proposed to perform under.

iii. The identification of <u>all</u> proposed LCATs (for both key and non-key positions AND the known optional growth support) and complete skill level descriptions from the ASB contract and any additional task specific supplemental requirements in terms of expertise (i.e. education) and experience (in terms of years of experience) that are being proposed to support task order performance. NOTE: If it is determined that varying skill levels (i.e. entry level, journeyman, junior, intermediate, senior, etc.) are required to efficiently support task order performance and the ASB LCATs are not inclusive of such varying levels, the contractor shall supplement the contract level LCATs to provide varying levels as required. The proposed utilization of supplemental skill level requirements shall include the establishment of varying skill levels and the corresponding labor rates. In no instance shall the proposed labor rates for the varying skill levels of the LCATs exceed the established ASB ceiling rate for the subject LCAT.

iv. The identification and description of the contractor's policies regarding retention, recruitment and benefits, to include the items listed below, that <u>will be applicable</u> to resultant task order. The proposal shall clearly address the "consistency" of said policies as applicable to staffing plans that include the utilization of joint ventures and subcontractors.

- Description of plans, methods, procedures and personnel that will be used to recruit employees.
- Description of the standard compensation package(s) that will be employed, including benefits, work week policy, and overtime policy. The discussion regarding benefits shall address extended vacations (those exceeding a one week duration). The discussion shall also identify and describe any innovative features of the compensation package, such as unusual benefits or bonuses. In addition, if applicable, the discussion shall include a description and explanation for the potential utilization of a non-standard compensation package for specific positions. Such positions shall also be identified.
- Description of how the salary structure recognizes the distinct differences in technical and supervisory skills (where applicable) and the complexity of varied disciplines as well as job difficulty.
- Description of how and when training will be provided to ensure retention of employees and to ensure employees remain current on the required skills.
- Description of methods to ensure qualifications of prospective employees, to include contractor conducted background investigations.
- Explanation of what extraordinary measures of recruiting will be taken to fill critical positions requiring unique or hard-to-fill technical expertise and who will have the authority to incur the expense.

- A description of the orientation provided to the employee (at no cost to the Government) prior to assignment to the task order.

3. Past Experience and Performance (part of the technical proposal) - The written past experience and performance section of the technical proposal shall be composed of the following:

a) The Government will consider the relevance of past performance information obtained in relation to the scope of this procurement. Past Performance, either positive or negative, which is considered by the Government to be more closely related to the scope of this effort will be given additional weight in the evaluation process.

b) Description of three (a total of three to include subcontractor references – additional past performance references will not be considered for evaluation purposes) past project references that demonstrate successful experience in the type of work requested in the PWS. Each reference shall provide a thorough explanation of it's relevant to the PWS. Each reference shall include the information bulleted below and shall be no more than two pages in length. The performance references shall be within the last three years.

Furthermore, the ASB prime contractor is required to include (within the three references identified above) at least one project supporting a Federal Agency that the ASB prime contractor performed ~~and completed~~ as the prime with an annual value, for each annual period of performance included within the project, of no less than $2 million. If the ASB prime contractor is a Joint Venture (JV) company that has no relevant past/present performance, which shall be clearly stated within the proposal, then the Government may consider one reference from one partner of the JV to meet the requirement in the preceding sentence regarding minimum performance requirements as a prime contractor. The removal of the word "completed" within the first sentence of this paragraph allows contractors to include current, on-going references/projects within the past performance submission; however, the Government reserves the right to give additional weight to completed past performance references/projects in the evaluation process.

i. Contracting agency/company and technical points of contact with their phone numbers, electronic-mail addresses, and titles.
ii. Contract number and delivery/task order number, as applicable.
iii. Contract type.
iv. The original contract award date (for the base period of performance) and the completion (or estimated completion) date (shall reflect all option periods).
v. Contract value (value of each performance period shall be identified).
vi. Number of contractor personnel involved.
vii. Identification of on/off site performance locations.
viii. Scope of work.

c) If applicable, the submittal in this section shall also list any contract or purchase order under which either a cure notice or show cause letter was received, or any contract or purchase order that was terminated for cause by the Government within the past three years. The contractor must briefly explain the facts and circumstances in each such instance.

d) The contractor is to provide the Past/Present Performance questionnaire included in the RFP as Attachment 3 to all performance references identified in the contractor's technical proposal for completion and direct submission to the GSA as instructed within the questionnaire. The date established for receipt of the questionnaires will be the same as the date and time established for receipt of the RFPs.

e) The Government may supplement the information from the Government's Past Performance Information Retreival System (PPIRS) for the prime and any proposed subcontractor firms. The Government may contact members of the acquisition workforce involved with previously awarded Federal contracts. The Government's contact with other members of the Government acquisition workforce, including Contracting Officer's, Contracting Officer Representatives (CORs), and Project Managers, can provide valuable insight and supplement the written PPIRS evaluations or provide insight into the contractor's performance of ongoing contracts.

f) Offerors with no relevant past or present performance history shall receive the rating of "neutral" meaning the rating is treated neither favorably nor unfavorably.

4. Price Submission - Use of RFP Attachment 2 is required. The price submission, excluding RFP Attachment 2, shall not exceed five pages.

a) Format. The contractor shall utilize the Government provided template, in the Government provided file format.

b) Core and Optional Growth Support. For informational purposes only, the Government estimate included 1,920 labor hours as the basis for a FTE position.

c) CLIN Structure. The Government reserves the right to award the support for each CLIN on an individual basis, to include both a FTE basis and a fractional FTE basis, contingent upon funding availability.

d) The Government's future actions and uncertainty regarding continuing need may result in the requirement to reduce the duration of support provided via the FFP FTE positions or fractional FTE positions (if proposed). As such, the Government hereby reserves the right to reduce the firm fixed price amount for each position based on a prorated calculation.

e) Travel. The Government's estimated travel cost for each performance period is listed in the Government provided template. The proposal shall identify any indirect cost related to the travel other direct costs. The proposal shall include a copy of the Defense Contract Audit Agency (DCAA) approval letter for any indirect rates (i.e. G&A, etc.).

f) Un-scheduled (work hour category D) Support. The contractor shall clearly identify all costs, other than the standard billable labor hours expended by contractor resources in direct support of such requirements, associated with support provided under work hour category D. The contractor shall propose and clearly describe a cost effective approach. If there are no additional costs other than the standard billable labor hours expended by contractor resources in direct support of such requirements, the contractor shall clearly state and indicate such within the price proposal.

g) The period of performance dates identified in the PWS are estimated dates. The actual performance dates for the base period may require revision, resulting in an earlier or a later start date. Price proposal revisions will be not required or considered if a revision to the base period of performance is required. All of the performance periods (Base Period, Option Periods 1, 2, 3 and 4) will each be for a period of 12 months, with each option period of performance reflecting the subsequent 12-month period following the preceding period.

V. EVALUATION CRITERIA AND SELECTION PROCESS

A. *General*

1. Evaluations will be conducted in accordance with the FAR Part 16.505(b).

2. GSA will determine best value to the Government based on evaluation of price and non-price factors considered. However, the Government will not issue an award at a significantly higher evaluated price to achieve only slightly superior performance capabilities. GSA will verify that proposed services are consistent with the contractor's GSA ASB contract.

B. *Evaluation Factors*

1. FACTOR 1: Technical Capability - The written Technical Capability submission composed of the Technical Approach, QCP and Staffing Approach/Plan. The items listed under this Technical Capability Factor ARE NOT sub factors and are not separately weighted for evaluation purposes. All items will be considered together for purposes of assigning a rating to this factor. The feasibility, extent, and quality of the contractor's technical capability will be evaluated based on the written submittal described in section IV(B)(2), above. The evaluation will be based on information pertaining to technical approach, and specifically focus on the breadth, depth and scope of the contractor's knowledge and understanding of the requirements described in this section. In addition, the relative quality and viability of the proposed staffing/labor mix/level of effort will be evaluated.

2. FACTOR 2: Past Experience and Performance - The Past Performance evaluation will include the references described in IV(B)(3), which may be verified by contacting references as deemed necessary by the Government along with past performance questionnaires, and will be evaluated based on the relevance of the information submitted. In rating this factor, GSA will consider the relevance in size and scope of each reference listed to the work described in this RFP. Past performance for projects similar in size and scope to the work described in this RFP may be given more weight in the evaluation. As such, the description of the work performed must be sufficiently detailed for the Government to make this determination.

3. FACTOR 3: Price – The Government will evaluate the realism and reasonableness of the proposed prices, rates, and number of labor hours, to determine overall best value. In addition, the Government will confirm that the rates proposed in the entire pricing proposal are accurate when compared to the contractor's current GSA ASB contract rates. Proposals containing inaccurate pricing information may be deemed ineligible for award and will not be further evaluated

VI. SELECTION

A. *Best Value Evaluation*

1. Proposals must demonstrate a clear understanding of the nature and scope of the work required. Failure to provide a realistic, reasonable, and complete proposal may reflect a lack of understanding of the requirements and may result in the proposal receiving no further evaluation and determined ineligible for award. Award will be established with the responsible contractor whose proposal conforms to the requirements outlined in this RFP and is most advantageous to the Government based on the best value determination.

2. The items listed under Technical Capability ARE NOT sub factors and are not separately weighted for evaluation purposes. All items will be considered together for purposes of assigning a rating to this factor.

3. The relative weights for the non-priced factors are listed in descending order of importance: Technical Capability and Past Experience and Performance. All non-priced factors combined are significantly more important than price.

4. Potential risk to the Government will also be evaluated. Technical and performance risk, based upon the proposer's evaluated technical capability and past performance experience, will be considered during the evaluation as well as any possible pricing risk and risks incurred as a result of the proposal assumptions.

B. *Discussions and Competitive Range*.

The Government intends to award a task order without discussion with respective contractors. The Government, however, reserves the right to conduct discussions if deemed in its best interest. The contracting officer may limit the number of proposals in the competitive range to the greatest number that will permit an efficient competition among the most highly rated proposals.

VII. ADDITIONAL TERMS AND CONDITIONS

The following clauses apply to this RFP and are provided by reference. The following clauses are incorporated with the same force and effect as if provided in full text:

FAR 52.212-4, Contract Terms and Conditions – Commercial Items (Dec 2014), Alternate I (May 2014)

FAR 52.217-5, Evaluation of Options (Jul 1990)

FAR 52.219-14, Limitations on Subcontracting (Nov 2011)

The following clauses are incorporated in full text:

FAR 52.217-8, Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor prior to expiration of the contract. (End of Clause)

FAR 52.217-9, Option to Extend the Term of the Contract (Mar 2000)

a) The Government may extend the term of this contract by written notice to the Contractor prior to expiration of the contract; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 60 months. (End of Clause)

GSA Special Clause: Limitation of Government's Obligation – Firm Fixed Price

Line items for Firm Fixed Price services may be incrementally funded. For these item(s), the sum of *** of the *** total price is presently available for payment and allotted to this task order award. An allotment schedule will be provided.

The Contractor agrees to perform up to the point at which the total amount payable by the Government, including reimbursement in the event of termination of those item(s) for the Government's convenience, approximates the total amount currently allotted to the contract. The Contractor is not authorized to continue work on those item(s) beyond that point. The Government will not be obligated in any event to reimburse the Contractor in excess of the amount allotted to the contract for those item(s) regardless of anything to the contrary in the clause entitled "Termination for Convenience of the Government." As used in this clause, the total amount payable by the Government in the event of termination of applicable contract line item(s) for convenience includes costs, profit, and estimated termination settlement costs for those item(s).

Notwithstanding the dates specified in the allotment schedule of this clause, the Contractor will notify the Contracting Officer in writing at least ninety days prior to the date when, in the Contractor's best judgment, the work will reach the point at which the total amount payable by the Government, including any cost for termination for convenience, will approximate 85 percent of the total amount then allotted to the contract for performance of the applicable item(s). The notification will state (1) the estimated date when that point will be reached and (2) an estimate of additional funding, if any, needed to continue performance of applicable line items up to the next scheduled date for allotment of funds identified in this clause, or to a mutually agreed upon substitute date. The notification will also advise the Contracting Officer of the estimated amount of additional funds that will be required for the timely performance of the item(s) funded pursuant to this clause, for a subsequent period as may be specified in the allotment schedule of this clause or otherwise agreed to by the parties. If after such notification additional funds are not allotted by the date identified in the Contractor's notification, or by an agreed substitute date, the Contracting Officer will terminate any item(s) for which additional funds have not been allotted, pursuant to the clause of this contract entitled "Termination for Convenience of the Government."

When additional funds are allotted for continued performance of the contract the parties will agree as to the period of contract performance which will be covered by the funds. The provisions of this clause will apply in like manner to the additional allotted funds and agreed substitute date, and the contract will be modified accordingly.

If, solely by reason of failure of the Government to allot additional funds, by the dates indicated below, in amounts sufficient for timely performance of the contract, the Contractor incurs additional costs or is delayed in the performance of the work under this contract and if additional funds are allotted, an equitable adjustment will be made in the price or prices (including appropriate target, billing, and ceiling prices where applicable) of the item(s), or in the time of delivery, or both. Failure to agree to any such equitable adjustment hereunder will be a dispute concerning a question of fact within the meaning of the clause entitled "Disputes."

The Government may at any time prior to termination allot additional funds for the performance of the contract.

The termination provisions of this clause do not limit the rights of the Government under the clause entitled "Default." The provisions of this clause are limited to the work and allotment of funds for the contract. This clause no longer applies once the contract is fully funded except with regard to the rights or obligations of the parties concerning equitable adjustments negotiated under this clause.

Nothing in this clause affects the right of the Government to terminate this contract pursuant to the clause of this contract entitled "Termination for Convenience of the Government."

Nothing in this clause shall be construed as authorization of voluntary services whose acceptance is otherwise prohibited under 31 U.S.C. 1342.

The parties contemplate that the Government will allot funds to this contract in accordance with the following schedule:

On execution of task order	***
Schedule To Be determined	***

*** To be inserted after negotiation/prior to task order award(s).
(End of clause)

VIII. RFP QUESTIONS

All questions resulting from the RFP shall be submitted in writing via e-mail to both individuals identified below no later than January 9th, 2015, 5:00 PM EST. All questions received will be consolidated and a response will be issued via a RFP amendment. Questions received after this date will not be considered

Yjuania Still
Contracting Officer
GSA/FAS
Phone: 618-622.5809
Email: yjuania.still@gsa.gov

Wendi Borrenpohl
Project Manager
GSA/FAS
Phone: 618.622.5806
Email: wendi.borrenpohl@gsa.gov

IX. DUE DATE

Electronic proposals must be submitted no later than the date established in the eBuy, with six hardcopies to be delivered no later than the first business day of this date/time, to:

GSA/FAS/5QZA
1710 Corporate Crossing, Suite 3
O'Fallon, IL 62269-3734

YJUANIA STILL
Contracting Officer

Attachments:

1. Performance Work Statement
2. Pricing Template
3. Past Performance Questionnaire

GSA e-Buy- Connect

My Rfqs | Close Connect Session

Modification Description

RFQ ID: RFQ949010 **Modification 5**

Date of Mod 5: 02/03/2015 06:05:16 PM EST

Description:
Amendment #5: Incorporates Clarification document (Q&A) and Revised RFP into the Solicitation. Added language in the RFP is highlighted in red. Closing date/time remains the same.

▷ Back

GSA RFQ949010 (GSA Task Id ID05140054)
Amendment #6

Clarification Document dated 2015.02.05

The purpose of this clarification document is to address questions submitted in response to the Request for Proposal (RFP), amendment #5. The questions have not been altered. The clarification document will be incorporated into the resultant task order award. Furthermore, the release of the subject clarification incorporates the items listed below into the RFP. The revisions hereby replace previous versions of the same documents in their entirety.

RFP 2015.02.05 – revision 3

No additional questions will be considered.

1. Regarding Amendment 5, Q&A answer #7 – If the identification page inserted within the plastic on the outside of the binder is not included within the established page limitation, would the same page be excluded from page count for soft copies?

   ***Answer**: Yes.*

2. If we have an ongoing contract which started six months ago , but has multiple periods of performance including base period at 6 months and option periods 1 through 4 at 12 month durations, and each option period after the six month base period (which is only period completed to date) will be over 2M in value --- Is that a qualified project or must there be at least 12 months of performance at 2M or greater in the prior three years. The prior answer to this question may not have considered that 6 month period referenced was only the base period of a multi-period/multi-year contract where the succeeding periods at 12 month duration would be over 2M?

   ***Answer**: The RFP requirements remain unchanged (excerpt included): "Furthermore, the ASB prime contractor is required to include (within the three references identified above) at least one project supporting a Federal Agency that the ASB prime contractor performed ~~and completed~~ as the prime with an annual value, for each annual period of performance included within the project, of no less than $2 million." A qualified project must meet the 12 month performance period at a dollar value of no less than $2 million. The 12 month performance period can be comprised of a base period and option period(s).*

3. Letter f) on page 9 in the RFP Amendment 5 version still states that "Offerors with no relevant past or present performance history shall receive the rating of "neutral" meaning the rating is treated neither favorably nor unfavorably." . Since this still remains and specifically allows for no past performance to be considered neutral, it is still unclear as to how letter f) should be interpreted versus the requirements in letter b) . Technically, letter f) still allows for responses with no relevant/ recent past performance to qualify and receive award. Please clarify the language if possible. While the response to question 183 reiterated the clarity of letter b) requirements, it did not specifically address the letter f) RFP statements?

   ***Answer**: Refer to paragraph (IV)(B)(3)(b) of the revised RFP . The items in paragraph (b) and (f) are unrelated as paragraph (f) is applicable solely to relevancy.*

REQUEST FOR PROPOSAL
ID05140054

In Support Of

CLIENT AGENCY:

United States Department of Agriculture (USDA)
National Information Technology Center (NITC)

PROJECT TITLE:

Information Technology Support

~~Original Version dated December 18, 2014~~

~~Revision 1 dated January 23, 2015~~

~~Revision 2 dated February 3, 2015~~

Revision 3 dated February 5, 2015

Table of Contents

I. INTRODUCTION 4

A. Performance Based Contracting Approach 4

B. Period of Performance 4

C. Level of Support 4

II. MINIMUM REQUIREMENTS - READ THIS FIRST 4

III. INSTRUCTIONS TO CONTRACTORS 5

A. Submission of Proposal 5

B. General Contractor Instructions 5

IV. PROPOSAL CONTENT 6

A. General 6

B. Detailed 6

1. Cover Letter 6
2. Technical Capability 7
3. Past Experience and Performance 9
4. Price Submission 10

V. EVALUATION CRITERIA AND SELECTION PROCESS 10

A. General 10

B. Evaluation Factors 11

1. FACTOR 1: Technical Capability 11
2. FACTOR 2: Past Experience and Performance 11
3. FACTOR 3: Price 11

VI. SELECTION 11

A. Best Value Evaluation 11

B. Discussions and Competitive Range. 11

VII. ADDITIONAL TERMS AND CONDITIONS 12

VIII.RFP QUESTIONS 13

IX. DUE DATE 14

DATE: February 5, 2015

MEMORANDUM FOR: General Services Administration (GSA)
Alliant Small Business (ASB)
Governmentwide Acquisition Contract (GWAC)

FROM: GSA
Federal Acquisition Service (FAS)
Acquisition Operations Division (5QZA)
1710 Corporate Crossing, Ste. #3
O'Fallon, IL 62269

SUBJECT: Request for Proposal (RFP) for GSA Order Number ID05140054

I. INTRODUCTION

It is the intent of the GSA FAS 5QZA to issue a single-award task order against the GSA ASB GWAC to provide a full range of Information Technology (IT) services in support of the United States Department of Agriculture (USDA), National Information Technology Center (NITC).

A. *Performance Based Contracting Approach*

This RFP utilizes a Performance Work Statement (PWS) (**RFP Attachment 1**) to provide the Government's overall desired outcomes/objectives for this requirement. The PWS provides the overall scope and general requirements. Specific task requirements are identified in **PWS Attachment A** via the utilization of Contract Line Item Number (CLIN) descriptions. The performance standards and acceptable quality levels are identified in both PWS Attachment A and **PWS Attachment B**, Labor Hour CLIN Service Delivery Summary, as applicable.

B. *Period of Performance*

The resulting task order will have a one-year base period and four, one-year option periods.

C. *Level of Support*

For indicating the scope of work only, the estimated core initial staffing levels in terms of Full-Time-Equivalent (FTE) positions are identified in **PWS Attachment C**. It is anticipated that the workload will fluctuate based on fluid schedule requirements; therefore, the contractor shall include provisions for optional growth support throughout the task order life cycle as reflected in the pricing template, which includes lump sum labor allotments for optional growth support that are equivalent to a percentage of the price/cost for the core requirements. To ensure maximum flexibility with respect to the optional growth support, the contractor shall include a complete price list identifying the proposed hourly labor rates for all ASB labor categories (LCATs), as reflected in the pricing template, that will be used as the pricing basis for all optional growth support. The actual time frame for the optional growth support implementation will be dependent upon actual scheduling requirements.

II. MINIMUM REQUIREMENTS - READ THIS FIRST

Contractor proposals submitted in response to this RFP must comply with the following minimum requirements. Proposals that fail to meet any ONE of these minimum requirements may be eliminated from further consideration and deemed ineligible for award.

- Submit complete information as required in these instructions.
- Comply with all requirements identified in these instructions.

- As detailed in section III, all electronic documents/data submitted must be enabled so that the text/data in those documents/data can be searched, highlighted, copied and pasted into other documents/spreadsheets as needed.
- The contractor shall utilize and fully complete the required pricing template (**RFP Attachment 2**). Contractor proposed labor rates shall not exceed the applicable contract ceiling rates.
- The contractor shall complete the registration process (contractor company, contractor company representatives, and ASB contract) for GSA's web-based procurement system, Information Technology Solutions Shop (ITSS). Contractors may contact the ITSS Registration Helpdesk at 877-243-2889, option #2, for registration assistance.

III. INSTRUCTIONS TO CONTRACTORS

A. *Submission of Proposal*

1. Proposals shall be received no later than the date identified in paragraph IX. Proposals received after this time will not be considered for award. All proposals shall be uploaded to eBuy (www.ebuy.gsa.gov) under the applicable RFP. Regarding page limitations, the documentation shall be single-spaced, Times New Roman font (no exceptions), no smaller than 11 point type-size, no less than 1 inch margins, that (if printed) would fit on 8 ½ x 11 inch paper. The only exception to the paper size (not an exception to the font requirements) is for the price proposal and the organizational chart. The price proposal shall be printed on paper of a sufficient size to allow each sheet within the pricing template to be printed on a single page. The organizational chart shall be printed on paper of sufficient size to allow the entire chart to be displayed on a single page.

2. The acceptable electronic formats are Adobe PDF or Microsoft Word except for pricing. Price proposals shall be submitted using the required pricing template. All Adobe PDF documents and Microsoft Word documents shall be submitted with the ability to highlight and copy the text/data of the document. Any documents submitted that are protected in such a way which does not enable the ability to highlight/copy/paste the text/data will not be accepted. All Microsoft Word documents shall be fully readable by Microsoft Office version 2007.

3. Pricing proposal information shall not contain any technical proposal information and vice versa. When uploading the proposal to eBuy, separate all pricing and technical proposal information into separate zip (winszip.exe) folders. The naming convention for the WinZip folders shall be as follows: for pricing "GS-06F-XXXXX PRICING.zip", for Technical "GS-06F-XXXXX TECH.zip" (Complete the X's with the GSA ASB contract number). Submit the cover letter as a standalone document with the same style of naming convention "GS-06F-XXXXX COVER LETTER." All past performance information shall be included within the "GS-06F-XXXXX TECH.zip" file.

4. As stated in Section IX, hard copies are also requested. Timeliness and responsiveness of the proposasl is first determined by the submission of the electronic proposal in eBuy, then followed by the delivery of the hard-copy proposals. Hard copy proposals are to be delivered to the address listed in paragraph IX no later than 24 hours following the close date/time identified in the same paragraph. Failure to meet both the eBuy submission and hard-copy submission deadlines will remove the proposal from consideration. The electronic submission will serve as the "official" submission.

B. *General Contractor Instructions*

1. Proposals shall clearly demonstrate an understanding of each of the Government's objectives and requirements.

2. A complete proposal shall consist of a cover letter; a technical proposal, including both a technical capability section and a past experience and performance section; and a price proposal as detailed below. Incomplete proposals will not be further evaluated and deemed ineligible for award.

3. Proposals submitted in any other way except as detailed in the submission of proposals section above will not be further evaluated and deemed ineligible for award.

4. Any proposal or proposal modification will not be accepted after the due date and time for proposals.

5. Any assumptions forming the basis of the proposal, whether technical or price related, must be clearly identified in the applicable proposal.

6. All proposals shall be handled in accordance with FAR Subpart 3.104, Procurement Integrity.

7. Information requested herein must be furnished in writing and be fully and completely in compliance with RFP instructions. The information requested and the manner of submission is essential to permit prompt evaluation of all proposals on a fair and uniform basis. Simple statements of compliance without the detailed description of how compliance will be accomplished may not be considered sufficient evidence that the contractor can meet the technical requirements.

8. Contractor employees responsible for preparing material that may be procurement sensitive/proprietary data must mark each page that the contractor believes contains such information with the legend "Proprietary Data".

IV. PROPOSAL CONTENT

A. *General*

1. Contractors should review the GSA ASB contract and are responsible for ensuring that proposals fully comply with all GSA ASB contract requirements. Each proposal shall clearly demonstrate that the contractor understands the PWS. The failure to explain the contractor's ability to meet all requirements may result in the contractor's proposal not being considered. Clarity and completeness of proposals are of the utmost importance. Therefore, proposals must be written in a practical, clear and concise manner.

2. The narrative shall provide the Government with a reasonable assurance that the contractor has the relevant experience, capacity and capability required to meet or exceed the requirements and Government objectives identified within the PWS. A mere restatement of the PWS will be deemed unacceptable and may result in the contractor being eliminated from further consideration and deemed ineligible for award.

3. Each proposal shall be legible, single-spaced, typewritten Times New Roman font (no exceptions), no smaller than 11 point type-size, no less than 1 inch margins, which can be printed on 8 ½ x 11 inch paper (with the exception of the price proposal and organizational chart as per paragraph (III)(A)(1)). Overall proposal content, excluding the pricing submission, complete labor category skill level descriptions, and stand-alone cover letter, shall be no more than 45 pages in length.

B. *Detailed*

1. Cover Letter - An authorized official who can obligate the contractor shall sign a Cover Letter in contractor format, on contractor letterhead, demonstrating the contractor's intent to be bound to the task order terms and conditions. This cover letter shall be no more than two (2) pages. The cover letter shall include:

   a) Alliant Small Business Contractor Company Name, Address, Contract Administration POC name/phone/email, Technical POC name/phone/email (if different than Contract Administration POC), CAGE, DUNS, TIN, Business Size, and GSA ASB Number.

   b) Subcontractor Information: The prime contractor shall also provide information on any subcontractor proposed. The cover letter shall identify and describe, in sufficient detail, any

proposed/potential sub-contractor agreements that may be required in the performance and completion of the task requirements.

2. Technical Capability (part of the technical proposal) - The written technical capability section of the technical proposal shall contain the following:

   a) Technical Approach

      i. Understanding and Methodology. The technical proposal shall include an overview of the methodology that will be utilized to guide the management and performance of the technical requirements identified in the PWS. The proposal shall include sufficient documentation to demonstrate both a detailed understanding of the stated requirements and the potential management challenges associated with the broad range of task areas involved. The technical proposal shall include a description of how the technical approach (i.e. description of the tasks to be performed) and analytical techniques will be applied to accomplish each of the requirements identified in the PWS.
      ii. Implementation. The technical approach shall include a phase-in plan to address the overall transition to the new task order, to include the recruitment and hiring of both new and incumbent contractor employees, and include sufficient documentation to demonstrate that the USDA will not experience a negative impact or disruption in service as a result from contractor personnel changes. The proposal shall identify all Government coordination that is anticipated to be required for the implementation. Detailed requirements for the phase-in plan are identified in PWS paragraph 8.7.1. If applicable, the phase-in plan shall clearly describe the contractor's proposed transition period, as defined in PWS paragraph 8.7.1., to include the following: specific duration of the transition period; detailed description of the proposed tasks to be completed during the transition period; and the identification of the resources proposed to complete such tasks during the transition period.

   b) Quality Control Plan (QCP). The plan shall include, but is not limited to the following:

      i. A description of the inspection system covering all services listed.
      ii. The inspection frequency.
      iii. The title of the individual(s) who shall perform the inspection and their organizational placement.
      iv. A description of the methods for identifying, correcting, and preventing defects in the quality of service performed before the level becomes unacceptable.

   c) Staffing Approach/Plan. The proposal shall include a complete staffing approach/plan that describes and illustrates the proposed utilization of contractor personnel resources and skill sets to perform and complete the PWS requirements. The staffing approach/plan shall include, at a minimum:

      i. An organization chart that depicts the complete staffing approach/plan and structure from the <u>head of the company to all individual performers/positions</u> (including key positions and non-key positions) proposed to support the resultant task order that demonstrates required personnel resources and skill sets via the identification of proposed labor categories for all individual performers/positions. The organization chart shall include the following:
         - A clear illustration of the operational relationships and task leadership among all entities, including all proposed joint venture team members and subcontractors, and the alignment of such entities. NOTE: The proposal shall include a narrative discussion identifying the roles and responsibilities of all proposed joint venture team members and subcontractors.
         - The identification of all proposed positions, to include the identification of all positions as either "key" or "non-key".

- The names of known individuals proposed to perform and fill positions. Positions to be filled by future identified proposed staffing shall be reflected by the use of "TBD" in lieu of a proper name.
- The United States (U.S.) citizenship status, if known, of all known individuals proposed to perform and fill positions. Positions to be filled by future identified proposed staffing shall also include such identification to illustrate the contractor's intent. In addition, the chart shall include the identification of the overall percentage, in numerical format, of proposed U.S. citizens and non-U.S. citizens.
- The name of the contractor company that will employ the individuals that staff all proposed positions.
- The identification of the physical locations for all proposed positions depicted on the chart.
- The identification of the proposed ASB labor category (LCAT) and PWS CLIN for all proposed positions.

ii. Resumes of proposed staffing for all key positions, which identify the education, certification, experience, background investigation status, and special skills of any individual(s) proposed to fill these positions as required by the applicable ASB LCAT. The resumes shall also include the identification of the experience, certifications, and expertise identified in the PWS as applicable and available. All resumes included within the proposal submission shall identify the proposed LCAT from the ASB contract and the PWS CLIN that the staffing member is being proposed to perform under.

iii. The identification of all proposed LCATs (for both key and non-key positions AND the known optional growth support) and complete skill level descriptions from the ASB contract and any additional task specific supplemental requirements in terms of expertise (i.e. education) and experience (in terms of years of experience) that are being proposed to support task order performance. NOTE: If it is determined that varying skill levels (i.e. entry level, journeyman, junior, intermediate, senior, etc.) are required to efficiently support task order performance and the ASB LCATs are not inclusive of such varying levels, the contractor shall supplement the contract level LCATs to provide varying levels as required. The proposed utilization of supplemental skill level requirements shall include the establishment of varying skill levels and the corresponding labor rates. In no instance shall the proposed labor rates for the varying skill levels of the LCATs exceed the established ASB ceiling rate for the subject LCAT.

iv. The identification and description of the contractor's policies regarding retention, recruitment and benefits, to include the items listed below, that will be applicable to resultant task order. The proposal shall clearly address the "consistency" of said policies as applicable to staffing plans that include the utilization of joint ventures and subcontractors.

- Description of plans, methods, procedures and personnel that will be used to recruit employees.
- Description of the standard compensation package(s) that will be employed, including benefits, work week policy, and overtime policy. The discussion regarding benefits shall address extended vacations (those exceeding a one week duration). The discussion shall also identify and describe any innovative features of the compensation package, such as unusual benefits or bonuses. In addition, if applicable, the discussion shall include a description and explanation for the potential utilization of a non-standard compensation package for specific positions. Such positions shall also be identified.
- Description of how the salary structure recognizes the distinct differences in technical and supervisory skills (where applicable) and the complexity of varied disciplines as well as job difficulty.
- Description of how and when training will be provided to ensure retention of employees and to ensure employees remain current on the required skills.
- Description of methods to ensure qualifications of prospective employees, to include contractor conducted background investigations.
- Explanation of what extraordinary measures of recruiting will be taken to fill critical positions requiring unique or hard-to-fill technical expertise and who will have the authority to incur the expense.

- A description of the orientation provided to the employee (at no cost to the Government) prior to assignment to the task order.

3. Past Experience and Performance (part of the technical proposal) - The written past experience and performance section of the technical proposal shall be composed of the following:

a) The Government will consider the relevance of past performance information obtained in relation to the scope of this procurement. Past Performance, either positive or negative, which is considered by the Government to be more closely related to the scope of this effort will be given additional weight in the evaluation process.

b) Description of three (a total of three to include subcontractor references – additional past performance references will not be considered for evaluation purposes) past project references that demonstrate successful experience in the type of work requested in the PWS. Each reference shall provide a thorough explanation of it's relevant to the PWS. Each reference shall include the information bulleted below and shall be no more than two pages in length. The performance references shall be within the last three years.

Furthermore, the ASB prime contractor is required to include (within the three references identified above) at least one project supporting a Federal Agency that the ASB prime contractor performed ~~and completed~~ as the prime with an annual value, for each annual period of performance included within the project, of no less than $2 million. If the ASB prime contractor is a Joint Venture (JV) company that has no relevant past/present performance, which shall be clearly stated within the proposal, then the Government may consider one reference from one partner of the JV to meet the requirement in the preceding sentence regarding minimum performance requirements as a prime contractor. The removal of the word "completed" within the first sentence of this paragraph allows contractors to include current, on-going references/projects within the past performance submission; however, the Government reserves the right to give additional weight to completed past performance references/projects in the evaluation process. The requirement contained in this paragraph is considered a minimum qualification requirement. Submissions that do not meet the requirements will NOT be further considered for award purposes.

i. Contracting agency/company and technical points of contact with their phone numbers, electronic-mail addresses, and titles.
ii. Contract number and delivery/task order number, as applicable.
iii. Contract type.
iv. The original contract award date (for the base period of performance) and the completion (or estimated completion) date (shall reflect all option periods).
v. Contract value (value of each performance period shall be identified).
vi. Number of contractor personnel involved.
vii. Identification of on/off site performance locations.
viii. Scope of work.

c) If applicable, the submittal in this section shall also list any contract or purchase order under which either a cure notice or show cause letter was received, or any contract or purchase order that was terminated for cause by the Government within the past three years. The contractor must briefly explain the facts and circumstances in each such instance.

d) The contractor is to provide the Past/Present Performance questionnaire included in the RFP as Attachment 3 to all performance references identified in the contractor's technical proposal for completion and direct submission to the GSA as instructed within the questionnaire. The date established for receipt of the questionnaires will be the same as the date and time established for receipt of the RFPs.

e) The Government may supplement the information from the Government's Past Performance Information Retreival System (PPIRS) for the prime and any proposed subcontractor firms. The Government may contact members of the acquisition workforce involved with previously awarded Federal contracts. The Government's contact with other members of the Government acquisition workforce, including Contracting Officer's, Contracting Officer Representatives (CORs), and Project Managers, can provide valuable insight and supplement the written PPIRS evaluations or provide insight into the contractor's performance of ongoing contracts.

f) Offerors with no relevant past or present performance history shall receive the rating of "neutral" meaning the rating is treated neither favorably nor unfavorably.

4. Price Submission - Use of RFP Attachment 2 is required. The price submission, excluding RFP Attachment 2, shall not exceed five pages.

a) Format. The contractor shall utilize the Government provided template, in the Government provided file format.

b) Core and Optional Growth Support. For informational purposes only, the Government estimate included 1,920 labor hours as the basis for a FTE position.

c) CLIN Structure. The Government reserves the right to award the support for each CLIN on an individual basis, to include both a FTE basis and a fractional FTE basis, contingent upon funding availability.

d) The Government's future actions and uncertainty regarding continuing need may result in the requirement to reduce the duration of support provided via the FFP FTE positions or fractional FTE positions (if proposed). As such, the Government hereby reserves the right to reduce the firm fixed price amount for each position based on a prorated calculation.

e) Travel. The Government's estimated travel cost for each performance period is listed in the Government provided template. The proposal shall identify any indirect cost related to the travel other direct costs. The proposal shall include a copy of the Defense Contract Audit Agency (DCAA) approval letter for any indirect rates (i.e. G&A, etc.).

f) Un-scheduled (work hour category D) Support. The contractor shall clearly identify all costs, other than the standard billable labor hours expended by contractor resources in direct support of such requirements, associated with support provided under work hour category D. The contractor shall propose and clearly describe a cost effective approach. If there are no additional costs other than the standard billable labor hours expended by contractor resources in direct support of such requirements, the contractor shall clearly state and indicate such within the price proposal.

g) The period of performance dates identified in the PWS are estimated dates. The actual performance dates for the base period may require revision, resulting in an earlier or a later start date. Price proposal revisions will be not required or considered if a revision to the base period of performance is required. All of the performance periods (Base Period, Option Periods 1, 2, 3 and 4) will each be for a period of 12 months, with each option period of performance reflecting the subsequent 12-month period following the preceding period.

V. EVALUATION CRITERIA AND SELECTION PROCESS

A. *General*

1. Evaluations will be conducted in accordance with the FAR Part 16.505(b).

2. GSA will determine best value to the Government based on evaluation of price and non-price factors considered. However, the Government will not issue an award at a significantly higher evaluated price

to achieve only slightly superior performance capabilities. GSA will verify that proposed services are consistent with the contractor's GSA ASB contract.

B. *Evaluation Factors*

1. FACTOR 1: Technical Capability - The written Technical Capability submission composed of the Technical Approach, QCP and Staffing Approach/Plan. The items listed under this Technical Capability Factor ARE NOT sub factors and are not separately weighted for evaluation purposes. All items will be considered together for purposes of assigning a rating to this factor. The feasibility, extent, and quality of the contractor's technical capability will be evaluated based on the written submittal described in section IV(B)(2), above. The evaluation will be based on information pertaining to technical approach, and specifically focus on the breadth, depth and scope of the contractor's knowledge and understanding of the requirements described in this section. In addition, the relative quality and viability of the proposed staffing/labor mix/level of effort will be evaluated.

2. FACTOR 2: Past Experience and Performance - The Past Performance evaluation will include the references described in IV(B)(3), which may be verified by contacting references as deemed necessary by the Government along with past performance questionnaires, and will be evaluated based on the relevance of the information submitted. In rating this factor, GSA will consider the relevance in size and scope of each reference listed to the work described in this RFP. Past performance for projects similar in size and scope to the work described in this RFP may be given more weight in the evaluation. As such, the description of the work performed must be sufficiently detailed for the Government to make this determination.

3. FACTOR 3: Price – The Government will evaluate the realism and reasonableness of the proposed prices, rates, and number of labor hours, to determine overall best value. In addition, the Government will confirm that the rates proposed in the entire pricing proposal are accurate when compared to the contractor's current GSA ASB contract rates. Proposals containing inaccurate pricing information may be deemed ineligible for award and will not be further evaluated

VI. SELECTION

A. *Best Value Evaluation*

1. Proposals must demonstrate a clear understanding of the nature and scope of the work required. Failure to provide a realistic, reasonable, and complete proposal may reflect a lack of understanding of the requirements and may result in the proposal receiving no further evaluation and determined ineligible for award. Award will be established with the responsible contractor whose proposal conforms to the requirements outlined in this RFP and is most advantageous to the Government based on the best value determination.

2. The items listed under Technical Capability ARE NOT sub factors and are not separately weighted for evaluation purposes. All items will be considered together for purposes of assigning a rating to this factor.

3. The relative weights for the non-priced factors are listed in descending order of importance: Technical Capability and Past Experience and Performance. All non-priced factors combined are significantly more important than price.

4. Potential risk to the Government will also be evaluated. Technical and performance risk, based upon the proposer's evaluated technical capability and past performance experience, will be considered during the evaluation as well as any possible pricing risk and risks incurred as a result of the proposal assumptions.

B. *Discussions and Competitive Range*.

The Government intends to award a task order without discussion with respective contractors. The Government, however, reserves the right to conduct discussions if deemed in its best interest. The contracting officer may limit the number of proposals in the competitive range to the greatest number that will permit an efficient competition among the most highly rated proposals.

VII. ADDITIONAL TERMS AND CONDITIONS

The following clauses apply to this RFP and are provided by reference. The following clauses are incorporated with the same force and effect as if provided in full text:

FAR 52.212-4, Contract Terms and Conditions – Commercial Items (Dec 2014), Alternate I (May 2014)

FAR 52.217-5, Evaluation of Options (Jul 1990)

FAR 52.219-14, Limitations on Subcontracting (Nov 2011)

The following clauses are incorporated in full text:

FAR 52.217-8, Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor prior to expiration of the contract. (End of Clause)

FAR 52.217-9, Option to Extend the Term of the Contract (Mar 2000)

a) The Government may extend the term of this contract by written notice to the Contractor prior to expiration of the contract; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 60 months. (End of Clause)

GSA Special Clause: Limitation of Government's Obligation – Firm Fixed Price

Line items for Firm Fixed Price services may be incrementally funded. For these item(s), the sum of *** of the *** total price is presently available for payment and allotted to this task order award. An allotment schedule will be provided.

The Contractor agrees to perform up to the point at which the total amount payable by the Government, including reimbursement in the event of termination of those item(s) for the Government's convenience, approximates the total amount currently allotted to the contract. The Contractor is not authorized to continue work on those item(s) beyond that point. The Government will not be obligated in any event to reimburse the Contractor in excess of the amount allotted to the contract for those item(s) regardless of anything to the contrary in the clause entitled "Termination for Convenience of the Government." As used in this clause, the total amount payable by the Government in the event of termination of applicable contract line item(s) for convenience includes costs, profit, and estimated termination settlement costs for those item(s).

Notwithstanding the dates specified in the allotment schedule of this clause, the Contractor will notify the Contracting Officer in writing at least ninety days prior to the date when, in the Contractor's best judgment, the work will reach the point at which the total amount payable by the Government, including any cost for termination for convenience, will approximate 85 percent of the total amount then allotted to the contract for performance of the applicable item(s). The notification will state (1) the estimated date when that point will be reached and (2) an estimate of additional funding, if any, needed to continue performance of applicable line items up to the next scheduled date for allotment of funds identified in this clause, or to a mutually agreed upon substitute date. The notification will also advise the Contracting Officer of the estimated amount of additional funds that will be required for the timely performance of the item(s) funded pursuant to this clause, for a subsequent period as may be specified in the allotment schedule of this clause or otherwise agreed to by the parties. If after such notification additional funds are not allotted by the date identified in the Contractor's notification, or by an agreed substitute date, the Contracting Officer will terminate any item(s) for which additional funds have not been allotted, pursuant to the clause of this contract entitled "Termination for Convenience of the Government."

When additional funds are allotted for continued performance of the contract the parties will agree as to the period of contract performance which will be covered by the funds. The provisions of this clause will apply in like manner to the additional allotted funds and agreed substitute date, and the contract will be modified accordingly.

If, solely by reason of failure of the Government to allot additional funds, by the dates indicated below, in amounts sufficient for timely performance of the contract, the Contractor incurs additional costs or is delayed in the performance of the work under this contract and if additional funds are allotted, an equitable adjustment will be made in the price or prices (including appropriate target, billing, and ceiling prices where applicable) of the item(s), or in the time of delivery, or both. Failure to agree to any such equitable adjustment hereunder will be a dispute concerning a question of fact within the meaning of the clause entitled "Disputes."

The Government may at any time prior to termination allot additional funds for the performance of the contract.

The termination provisions of this clause do not limit the rights of the Government under the clause entitled "Default." The provisions of this clause are limited to the work and allotment of funds for the contract. This clause no longer applies once the contract is fully funded except with regard to the rights or obligations of the parties concerning equitable adjustments negotiated under this clause.

Nothing in this clause affects the right of the Government to terminate this contract pursuant to the clause of this contract entitled "Termination for Convenience of the Government."

Nothing in this clause shall be construed as authorization of voluntary services whose acceptance is otherwise prohibited under 31 U.S.C. 1342.

The parties contemplate that the Government will allot funds to this contract in accordance with the following schedule:

On execution of task order	***
Schedule To Be determined	***

*** To be inserted after negotiation/prior to task order award(s).
(End of clause)

VIII. RFP QUESTIONS

All questions resulting from the RFP shall be submitted in writing via e-mail to both individuals identified below no later than January 9th, 2015, 5:00 PM EST. All questions received will be consolidated and a response will be issued via a RFP amendment. Questions received after this date will not be considered

Yjuania Still
Contracting Officer
GSA/FAS

Wendi Borrenpohl
Project Manager
GSA/FAS

Phone: 618-622.5809 Phone: 618.622.5806
Email: yjuania.still@gsa.gov Email: wendi.borrenpohl@gsa.gov

IX. DUE DATE

Electronic proposals must be submitted no later than the date established in the eBuy, with six hardcopies to be delivered no later than the first business day of this date/time, to:

GSA/FAS/5QZA
1710 Corporate Crossing, Suite 3
O'Fallon, IL 62269-3734

YJUANIA STILL
Contracting Officer

Attachments:

1. Performance Work Statement
2. Pricing Template
3. Past Performance Questionnaire

GSA e-Buy- Connect

My Rfqs | Close Connect Session

Modification Description

RFQ ID: RFQ949010 **Modification 6**

Date of Mod 6: 02/05/2015 02:03:40 PM EST

Description:
Amendment #6: Incorporates Clarification document (Q&A) and Revised RFP into the Solicitation. Added language in the RFP is highlighted in red. Closing date/time remains the same.

▷ Back